



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

500.39847X00

Applicant(s): CH. OKAMOTO, ET AL
Serial No.: 09 / 801,748
Filed: MARCH 9, 2001
Title: "IDENTIFICATION CODE MANAGEMENT METHOD AND
MANAGEMENT SYSTEM".

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

MARCH 29, 2001

Sir:

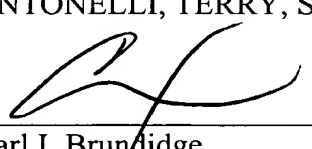
Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s)
the right of priority based on:

Japanese Patent Application No. 2000 - 210689
Filed: JULY 6, 2000

A certified copy of said Japanese Patent Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP



Carl I. Brundidge
Registration No. 29,621

CIB/rp
Attachment



日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 7月 6日

出 願 番 号

Application Number:

特願2000-210689

出 願 人

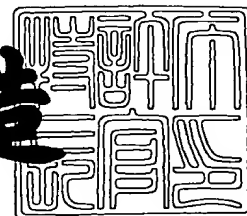
Applicant (s):

株式会社日立製作所

2001年 3月16日

特 許 庁 長 官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2001-3020089

【書類名】 特許願

【整理番号】 K00009671

【提出日】 平成12年 7月 6日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 19/00

【請求項の数】 42

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

 【氏名】 岡本 周之

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

 【氏名】 宝木 和夫

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

 【氏名】 福澤 寧子

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社日立製作所

【代理人】

 【識別番号】 100075096

 【弁理士】

 【氏名又は名称】 作田 康夫

【手数料の表示】

 【予納台帳番号】 013088

 【納付金額】 21,000円

【提出物件の目録】

【物件名】	明細書	1
【物件名】	図面	1
【物件名】	要約書	1
【プルーフの要否】	要	

【書類名】 明細書

【発明の名称】 I D の管理方法及び管理システム

【特許請求の範囲】

【請求項 1】

ID発行の受注を行なうID受注端末と、前記IDが格納されたIDタグの製造を行なう製造工場用端末と、ネットワークを介して前記ID受注端末および製造工場用端末に接続されたID管理端末とを含むID管理システムを用いて、IDの管理を行うID管理方法であって、

前記IDタグには、外部からデータを読み取り可能な電子回路チップが装着されており、

前記電子回路チップは、書き換え不可の記憶領域を有し、且つ当該領域に、外部から読み取り可能なデータとして、受注したIDと、IDの属性情報と、改竄検知符号、とを含む、拡張IDを格納しており、

前記ID管理端末において、

前記ID受注端末から、前記拡張IDを含む受注ID登録要求が送られてきた場合に、当該拡張IDが登録済みであるとして、データベースに登録する受注ID登録ステップと、

前記製造工場用端末から、製造済みの前記IDタグに格納されている前記拡張IDを含む、製造済みID登録要求が送られてきた場合に、当該拡張IDを格納した前記IDタグが製造済みであるとして、前記データベースに登録する製造済みID登録ステップと、を有するID管理方法。

【請求項 2】

請求項 1 記載のID管理方法であって、

前記ID管理端末において、

前記ID受注端末から、前記拡張IDを含むID重複確認要求が送られてきた場合に、当該拡張IDが受注済みであるとして前記データベースに登録されているか否かを調べ、

その結果を前記ID受注端末に通知するID重複確認ステップをさらに有するID管理方法。

【請求項 3】

請求項 1 記載の ID 管理方法であって、

前記 ID 管理端末において、

前記 ID タグ 製造工場用 端末から、前記 ID タグ に格納されている前記 拡張 ID を含む、欠番 ID 登録要求が送られてきた場合に、当該要求に含まれる 拡張 ID が欠番 ID であるとして、前記 データベース に登録する欠番 ID 登録ステップをさらに有する ID 管理方法。

【請求項 4】

請求項 1 記載の ID 管理方法であって、

前記 ID 管理システムは、

ネットワークを介して前記 ID 管理端末に接続された、ID 利用端末を含んでおり

前記 ID 管理端末において、

前記 ID 利用端末から、前記 拡張 ID を含む検証要求が送られてきた場合に、当該 拡張 ID を、データベースに格納してある 拡張 ID と比較し、送られてきた 拡張 ID に含まれる前記 改竄検知符号が正当か否かを検証する検証ステップをさらに有する ID 管理方法。

【請求項 5】

請求項 1 記載の ID 管理方法であって、

前記 ID 管理システムは、

ネットワークを介して前記 ID 管理端末に接続された、ID 利用端末を含んでおり

前記 ID 管理端末において、

前記 ID 利用端末から、前記 ID の属性情報を含む検証用鍵要求が送られてきた場合に、当該属性情報と対応づけられてデータベースに格納してある、前記 改竄検知符号の検証用の鍵を、前記 ID 利用端末に送信するステップをさらに有する ID 管理方法。

【請求項 6】

請求項 1 記載の ID 管理方法であって、

前記ID管理システムは、

ネットワークを介して前記ID管理端末に接続された、ID利用端末を含んでおり

前記ID管理端末において、

前記ID利用端末から、復号化用鍵要求が送られてきた場合に、データベースに格納してある、暗号化された拡張IDの復号化用の鍵を、前記ID利用端末に送信するステップをさらに有するID管理方法。

【請求項 7】

請求項 1 記載のID管理方法であって、

前記ID管理システムは、

ネットワーク 2 を介して前記ID管理端末に接続された、ID利用端末を含んでおり、

前記ID管理端末において、

前記ID利用端末から、前記拡張IDを含む、失効ID登録要求が送られてきた場合に、当該要求に含まれる拡張IDが失効IDであるとして、前記データベースに登録する失効ID登録ステップをさらに有するID管理方法。

【請求項 8】

請求項 1 記載のID管理方法であって、

前記ID管理システムは、

ネットワークを介して前記ID受注端末に接続された、顧客端末を含んでおり、

前記ID受注端末において、

前記顧客端末から、前記IDタグを発注する顧客の情報と、前記IDタグへの格納を希望するIDと、前記IDの改竄検知符号を生成するための鍵と、を含む発注情報が送られてきた場合に、当該発注情報を用いて、前記IDの属性情報と、前記改竄検知符号と、を生成し、前記拡張IDを生成する拡張ID生成ステップと、

前記顧客端末からの要求に応じて、前記発注情報と、前記拡張IDと、を含む受注情報を送信するステップと、

前記受注情報を含む受注ID登録要求をID管理端末に送信する受注ID登録要求ステップと、

前記拡張IDを含むIDタグ製造要求を前記IDタグ製造工場用端末に送信するIDタグ製造要求ステップと、を有するID管理方法。

【請求項 9】

請求項 1 記載のID管理方法であって、
前記IDタグ製造工場用端末において、
前記ID受注端末から、前記拡張IDを含むIDタグ製造要求が送られてきた場合に、前記IDタグを製造させるステップと、
製造された前記IDタグを検査させるステップと、
前記検査ステップの結果が合格の場合に、前記IDタグに格納されている前記拡張IDを含む、製造済みID登録要求を前記ID管理端末に送信する製造済みID登録要求ステップと、を有するID管理方法。

【請求項 1 0】

請求項 1 記載のID管理方法であって、
前記ID利用端末において、
処理動作の指示を受け入れる指示入力ステップと、
前記IDタグに装着されている前記電子回路チップから前記拡張IDを取得するID読み取りステップと、
前記読み取りステップで取得した前記拡張IDの正当性を、当該拡張IDに含まれる前記改竄検知符号を用いて検証する検証ステップと、
前記指示入力ステップで受け入れた指示が情報読取指示である場合に、前記ID読み取りステップで取得した前記拡張IDと対応づけられている情報をデータベースから取り出し、当該情報に応じて定められた処理を行なうステップと、
前記指示入力ステップで受け入れた指示が更新指示である場合に、更新情報を入手し、当該更新情報で、前記ID読み取りステップで取得した前記拡張IDと対応づけられている情報を更新するステップと、
前記指示入力ステップで受け入れた指示が新規登録指示である場合に、新規情報を入手し、当該新規情報を、前記ID読み取りステップで取得した前記拡張IDと対応づけてデータベースに格納するステップと、
前記指示入力ステップで受け入れた指示が失効ID登録指示である場合に、前

記IDタグの情報と対応づけられている前記拡張IDをデータベースから取り出し、当該拡張IDを含む失効ID登録要求をID管理端末に送信する失効ID登録要求ステップと、

を有するID管理方法。

【請求項11】

ID発行の受注を行なうID受注端末と、前記IDが格納されたIDタグの製造を行なう製造工場用端末と、ネットワークを介して前記ID受注端末および製造工場用端末に接続されたID管理端末とを含むID管理システムであって、

前記IDタグは、外部からデータを読み取り可能な電子回路チップを備え、

前記電子回路チップは、書き換え不可の記憶領域を有し、且つ当該領域に、外部から読み取り可能なデータとして、受注したIDと、IDの属性情報と、改竄検知符号、とを含む、拡張IDを格納しており、

前記ID受注端末は、受注時に受け入れた発注情報から生成した受注情報を含む受注ID登録要求を、前記ID管理端末に送る受注ID登録要求処理部を備え、

前記ID管理端末は、前記受注ID登録要求が送られてきた場合に、当該拡張IDが登録済みであるとして、データベースに登録する受注ID登録処理部を備え、

前記製造工場用端末は、製造済みの前記IDタグに格納されている前記拡張IDを含む、製造済みID登録要求を、前記ID管理端末に送らせる製造済みID登録要求処理部を備え、

前記ID管理端末は、前記製造済みID登録要求が送られてきた場合に、当該拡張IDを格納した前記IDタグが製造済みであるとして、前記データベースに登録する製造済みID登録処理部を備えるID管理システム。

【請求項12】

請求項11記載のID管理システムであって、

前記ID管理端末において、

前記ID受注端末から、前記拡張IDを含むID重複確認要求が送られてきた場合に、当該拡張IDが受注済みであるとして前記データベースに登録されているか否かを調べ、

その結果を前記ID受注端末に通知するID重複確認処理部をさらに有するID管理シ

ステム。

【請求項 1 3】

請求項 1 1 記載のID管理システムであって、

前記ID管理端末において、

前記IDタグ製造工場用端末から、前記IDタグに格納されている前記拡張IDを含む、欠番ID登録要求が送られてきた場合に、当該要求に含まれる拡張IDが欠番IDであるとして、前記データベースに登録する欠番ID登録処理部をさらに有するID管理システム。

【請求項 1 4】

請求項 1 1 記載のID管理システムであって、

前記ID管理システムは、

ネットワークを介して前記ID管理端末に接続された、ID利用端末を含んでおり

前記ID管理端末において、

前記ID利用端末から、前記拡張IDを含む検証要求が送られてきた場合に、当該拡張IDを、データベースに格納してある拡張IDと比較し、送られてきた拡張IDに含まれる前記改竄検知符号が正当か否かを検証する検証処理部をさらに有するID管理システム。

【請求項 1 5】

請求項 1 1 記載のID管理システムであって、

前記ID管理システムは、

ネットワークを介して前記ID管理端末に接続された、ID利用端末を含んでおり

前記ID管理端末において、

前記ID利用端末から、前記IDの属性情報を含む検証用鍵要求が送られてきた場合に、当該属性情報と対応づけられてデータベースに格納してある、前記改竄検知符号の検証用の鍵を、前記ID利用端末に送信する処理部をさらに有するID管理システム。

【請求項 1 6】

請求項 1 1 記載の ID 管理システムであって、

前記 ID 管理システムは、

ネットワークを介して前記 ID 管理端末に接続された、ID 利用端末を含んでおり

前記 ID 管理端末において、

前記 ID 利用端末から、復号化用鍵要求が送られてきた場合に、データベースに格納してある、暗号化された拡張 ID の復号化用の鍵を、前記 ID 利用端末に送信する処理部をさらに有する ID 管理システム。

【請求項 1 7】

請求項 1 1 記載の ID 管理システムであって、

前記 ID 管理システムは、

ネットワーク 2 を介して前記 ID 管理端末に接続された、ID 利用端末を含んでおり、

前記 ID 管理端末において、

前記 ID 利用端末から、前記拡張 ID を含む、失効 ID 登録要求が送られてきた場合に、当該要求に含まれる拡張 ID が失効 ID であるとして、前記データベースに登録する失効 ID 登録処理部をさらに有する ID 管理システム。

【請求項 1 8】

請求項 1 1 記載の ID 管理システムであって、

前記 ID 管理システムは、

ネットワークを介して前記 ID 受注端末に接続された、顧客端末を含んでおり、

前記 ID 受注端末において、

前記顧客端末から、前記 ID タグを発注する顧客の情報と、前記 ID タグへの格納を希望する ID と、前記 ID の改竄検知符号を生成するための鍵と、を含む発注情報が送られてきた場合に、当該発注情報を用いて、前記 ID の属性情報と、前記改竄検知符号と、を生成し、前記拡張 ID を生成する拡張 ID 生成処理部と、

前記顧客端末からの要求に応じて、前記発注情報と、前記拡張 ID と、を含む受注情報を送信する受注情報送信処理部と、

前記受注情報を含む受注ID登録要求をID管理端末に送信する受注ID登録要求処理部と、

前記拡張IDを含むIDタグ製造要求を前記IDタグ製造工場用端末に送信するIDタグ製造要求処理部と、を有するID管理システム。

【請求項 1 9】

請求項 1 1 記載のID管理システムであって、

前記IDタグ製造工場用端末は、

前記ID受注端末から、前記拡張IDを含むIDタグ製造要求が送られてきた場合に、前記IDタグの製造と、

製造された前記IDタグの検査を指示する制御部と、

前記検査処理部の結果が合格の場合に、前記IDタグに格納されている前記拡張IDを含む、製造済みID登録要求を前記ID管理端末に送信する製造済みID登録要求処理部と、を有するID管理システム。

【請求項 2 0】

請求項 1 1 記載のID管理システムであって、

前記ID利用端末において、

処理動作の指示を受け入れる指示入力処理部と、

前記IDタグに装着されている前記電子回路チップから前記拡張IDを取得するID読み取り処理部と、

前記読み取り処理部で取得した前記拡張IDの正当性を、当該拡張IDに含まれる前記改竄検知符号を用いて検証する検証処理部と、

前記指示入力処理部で受け入れた指示が情報読取指示である場合に、前記ID読み取り処理部で取得した前記拡張IDと対応づけられている情報をデータベースから取り出し、当該情報に応じて定められた処理を行なう処理部と、

前記指示入力処理部で受け入れた指示が更新指示である場合に、更新情報を入手し、当該更新情報で、前記ID読み取り処理部で取得した前記拡張IDと対応づけられている情報を更新する処理部と、

前記指示入力処理部で受け入れた指示が新規登録指示である場合に、新規情報を入手し、当該新規情報を、前記ID読み取り処理部で取得した前記拡張IDと対応

づけてデータベースに格納する処理部と、

前記指示入力ステップで受け入れた指示が失効ID登録指示である場合に、前記IDタグの情報と対応づけられている前記拡張IDをデータベースから取り出し、当該拡張IDを含む失効ID登録要求をID管理端末に送信する処理部と、を有するID管理システム。

【請求項 2 1】

ネットワークに接続されて用いられ、IDタグに格納された拡張IDの管理を行うID管理端末であって、

前記IDタグは、外部からデータを読み取り可能な、書き換え不可の記憶領域を有し、且つ当該領域に、受注したIDと、IDの属性情報と、改竄検知符号、とを含む、拡張IDを格納しており、

前記拡張IDと、当該拡張IDに関連する情報と、を登録するデータベースを記憶する記憶手段と、

前記ネットワークに接続された他の端末と、通信を行う通信手段と、

前記通信手段により、前記他の端末から、受注時に受け入れた発注情報から生成した受注情報を含む受注ID登録要求が送られてきた場合に、当該拡張IDが登録済みであるとして、データベースに登録する受注ID登録手段と、

前記通信手段により、前記他の端末から、製造済みの前記IDタグに格納されている前記拡張IDを含む、製造済みID登録要求が送られてきた場合に、当該拡張IDを格納した前記IDタグが製造済みであるとして、前記データベースに登録する製造済みID登録手段と、を有するID管理端末。

【請求項 2 2】

請求項 2 1 記載のID管理端末であって、

前記通信手段により、前記他の端末から、前記拡張IDを含むID重複確認要求が送られてきた場合に、当該拡張IDが受注済みであるとして前記データベースに登録されているか否かを調べるID重複確認手段をさらに有し、

前記通信手段は、

前記ID重複確認手段での確認結果を前記他の端末に送信するID管理端末。

【請求項 2 3】

請求項 2 1 記載の ID 管理端末であって、

前記通信手段により、前記他の端末から、前記 ID タグに格納されている前記拡張 ID を含む、欠番 ID 登録要求が送られてきた場合に、当該拡張 ID が欠番 ID であるとして、前記データベースに登録する欠番 ID 登録手段をさらに有する ID 管理端末。

【請求項 2 4】

請求項 2 1 記載の ID 管理端末であって、

前記通信手段により、前記他の端末から、前記拡張 ID を含む検証要求が送られてきた場合に、当該拡張 ID を、データベースに格納してある拡張 ID と比較し、送られてきた拡張 ID に含まれる前記改竄検知符号が正当か否かを検証する検証手段をさらに有し、

前記通信手段は、

前記検証手段での検証結果を前記他の端末に送信する ID 管理端末。

【請求項 2 5】

請求項 2 1 記載の ID 管理端末であって、

前記通信手段により、前記他の端末から、前記 ID の属性情報を含む検証用鍵要求が送られてきた場合に、当該属性情報と対応づけられてデータベースに格納してある、前記改竄検知符号の検証用の鍵を入手する検証用鍵入手手段をさらに有し、

前記通信手段は、

前記改竄検知符号の検証用の鍵を前記端末に送信する ID 管理端末。

【請求項 2 6】

請求項 2 1 記載の ID 管理端末であって、

前記通信手段により、前記他の端末から、復号化用鍵要求が送られてきた場合に、データベースに格納してある、暗号化された拡張 ID の復号化用の鍵を入手する復号化用鍵入手手段をさらに有し、

前記通信手段は、

前記暗号化された拡張 ID の復号化用の鍵を前記端末に送信する ID 管理端末。

【請求項 2 7】

請求項 2 1 記載の ID 管理端末であって、

前記通信手段により、前記他の端末から、前記拡張 ID を含む失効 ID 登録要求が送られてきた場合に、当該要求に含まれる拡張 ID が失効 ID であるとして、前記データベースに登録する失効 ID 登録手段をさらに有する ID 管理端末。

【請求項 2 8】

ネットワークに接続されて用いられ、ID タグに格納される ID の発行を受注する ID 受注端末であって、

前記 ID タグには、外部からデータを読み取り可能な、書き換え不可の記憶領域を有し、且つ当該領域に、受注した ID と、ID の属性情報と、改竄検知符号、とを含む、拡張 ID を格納しており、

前記ネットワークに接続された他の端末と、通信を行う通信手段と、

前記他の端末から、前記 ID タグを発注する顧客の情報と、前記 ID タグへの格納を希望する ID と、前記 ID の改竄検知符号を生成するための鍵と、を含む発注情報が送られてきた場合に、当該発注情報を用いて、前記 ID の属性情報と、前記改竄検知符号と、を生成し、前記拡張 ID を生成する拡張 ID 生成部と、

前記通信手段により、前記発注情報から生成した受注情報を含む受注 ID 登録要求を ID 管理端末に送信する受注 ID 登録要求手段と、

前記通信手段により、前記拡張 ID を含む ID タグ製造要求を前記 ID タグ製造工場用端末に送信する ID タグ製造要求手段と、を有する ID 受注端末。

【請求項 2 9】

請求項 2 8 記載の ID 受注端末であって、

前記通信手段により、前記拡張 ID を含む ID 重複確認要求を前記他の端末に送信して、前記拡張 ID が前記 ID 管理端末に登録してある拡張 ID と重複しているか否かを確認させる ID 重複確認要求処理部をさらに有する ID 受注端末。

【請求項 3 0】

請求項 2 8 記載の ID 受注端末であって、

乱数を生成し、当該乱数を前記改竄検知符号の生成用の鍵とする手段をさらに有する ID 受注端末。

【請求項 3 1】

請求項 2 8 記載の ID 受注端末であって、

前記拡張 ID を暗号化し、暗号化してあることを示す暗号化符号を添付する手段をさらに有する ID 受注端末。

【請求項 3 2】

ネットワークに接続されて用いられ、ID タグを製造する ID タグ製造工場で用いる ID タグ製造工場用端末であって、

前記 ID タグは、外部からデータを読み取り可能な、書き換え不可の記憶領域を有し、且つ当該領域に、受注した ID と、ID の属性情報と、改竄検知符号、とを含む、拡張 ID を格納しており、

前記ネットワークに接続された他の端末と、通信を行う通信手段と、

前記通信手段により、前記他の端末から、前記拡張 ID を含む ID タグ製造要求が送られてきた場合に、当該製造要求に従った前記 ID タグの製造と、製造された前記 ID タグの検査を実施させる制御手段と、

前記検査の結果が合格の場合に、前記通信手段により、前記 ID タグに格納されている前記拡張 ID を含む、製造済み ID 登録要求を前記他の端末に送信して、当該他の端末に、前記拡張 ID を格納した ID タグが製造済みであるとして登録させる製造済み ID 登録要求手段と、

を有する ID タグ製造工場用端末。

【請求項 3 3】

請求項 3 2 記載の ID タグ製造工場用端末であって、

前記検査の結果が不合格であり、かつ、前記 ID タグの再製造が不要な場合に、前記通信手段により、前記 ID タグに格納されている前記拡張 ID を含む、欠番 ID 登録要求を前記他の端末に送信して、当該他の端末に、前記拡張 ID が欠番 ID であるとして登録させる欠番 ID 登録要求手段をさらに有する ID タグ製造工場用端末。

【請求項 3 4】

ネットワークに接続されて用いられ、ID タグを利用する際に用いる ID 利用端末であって、

前記 ID タグには、外部からデータを読み取り可能な、書き換え不可の記憶領域を

有し、且つ当該領域に、受注したIDと、IDの属性情報と、改竄検知符号、とを含む、拡張IDを格納しており、

前記拡張IDと、当該拡張IDに関連する情報と、当該拡張IDが格納されている前記IDタグと対応づけられている情報と、を登録するデータベースを記憶する記憶手段と、

前記ネットワークに接続された、前記他の端末と通信を行う通信手段と、

処理動作の指示を受け入れる指示入力手段と、

前記IDタグに装着されている前記電子回路チップから前記拡張IDを取得するID読み取り手段と、

前記読み取り手段で取得した前記拡張IDの正当性を、当該拡張IDに含まれる前記改竄検知符号を用いて検証する検証手段と、

前記指示入力手段で受け入れた指示が情報読取指示である場合に、前記ID読み取り手段で取得した前記拡張IDと対応づけられている情報をデータベースから取り出し、当該情報に応じて定められた処理を行なう手段と、

前記指示入力手段で受け入れた指示が更新指示である場合に、更新情報を入手し、当該更新情報で、前記ID読み取り手段で取得した前記拡張IDと対応づけられている情報を更新する手段と、

前記指示入力手段で受け入れた指示が新規登録指示である場合に、新規情報を入手し、当該新規情報を、前記ID読み取り手段で取得した前記拡張IDと対応づけてデータベースに格納する手段と、

前記指示入力手段で受け入れた指示が失効ID登録指示である場合に、前記IDタグの情報と対応づけられている前記拡張IDをデータベースから取り出し、当該拡張IDを含む失効ID登録要求をID管理端末に送信する手段と、

を有するID利用端末。

【請求項 3 5】

請求項 3 4 記載のID利用端末であって、

前記ID読み取り手段で取得した前記拡張IDが暗号化されている場合に、前記記憶手段に格納されている復号化用の鍵を用いて復号化を行なう手段をさらに有するID利用端末。

【請求項 3 6】

請求項 3 4 記載の ID 利用端末であって、

前記 ID 読み取り手段で取得した前記拡張 ID が暗号化されており、かつ、前記記憶手段に復号化用の鍵を所有していない場合に、前記通信手段により、復号化用鍵要求を前記他の端末に送信して、当該他の端末に、前記復号化用の鍵を送信させる手段をさらに有する ID 利用端末。

【請求項 3 7】

請求項 3 4 記載の ID 利用端末であって、

前記 ID 読み取り手段で取得した前記拡張 ID に含まれる前記改竄検知符号を検証する鍵を所有していない場合に、前記通信手段により、前記拡張 ID を含む検証用鍵要求を前記他の端末に送信して、当該他の端末に、前記検証用鍵を送信させる手段をさらに有する ID 利用端末。

【請求項 3 8】

請求項 3 4 記載の ID 利用端末であって、

前記通信手段により、前記 ID 読み取り手段で取得した前記拡張 ID を含む、検証要求を前記他の端末に送信して、当該他の端末に、前記拡張 ID の正当性を検証させる検証要求手段をさらに有し、

前記検証手段は、

検証結果として、前記他の端末から送られてくる前記検証要求に対する結果を用いる ID 利用端末。

【請求項 3 9】

ネットワークに接続可能な複数の計算機に、ID 発行の受注を行なう ID 受注端末と、前記 ID が格納された ID タグの製造を行なう製造工場用端末と、ID 管理端末とからなる ID 管理システムを実現させるプログラム製品であって、

前記計算機が読みとり可能な媒体と、

前記 ID 受注端末となる前記計算機に、受注時に受け入れた発注情報から生成した受注情報を含む受注 ID 登録要求を、前記 ID 管理端末に送らせる受注 ID 登録要求処理部を実現させるモジュールと、

前記 ID 管理端末となる前記計算機に、前記受注 ID 登録要求が送られてきた場合

に、当該拡張IDが登録済みであるとして、データベースに登録する受注ID登録処理部を実現させるモジュールと、

前記製造工場用端末となる前記計算機に、製造済みの前記IDタグに格納されている前記拡張IDを含む、製造済みID登録要求を、前記ID管理端末に送らせる製造済みID登録要求処理部を実現させるモジュールと、

前記ID管理端末となる前記計算機に、前記製造済みID登録要求が送られてきた場合に、当該拡張IDを格納した前記IDタグが製造済みであるとして、前記データベースに登録する製造済みID登録処理部を実現させるモジュールと、を備えるプログラム製品。

【請求項 4 0】

流通を管理するためのIDタグを備える物品であって、

前記IDタグは、前記物品のIDと前記物品に関わる属性情報と、前記IDと前記属性情報に対する改竄検知符号とからなる拡張IDを格納し、

前記IDと、前記属性情報と、前記改竄検知符号と、前記改竄検知符号の検証用の鍵を、関連付けて格納するデータベースを用いて、前記拡張IDの正当性を確認可能としたIDタグを備える物品。

【請求項 4 1】

請求項 4 0 記載のIDタグを備える物品であって、

前記拡張IDは、さらに、前記IDと前記属性情報との割り当てを制御するクラス情報をさらに含むIDタグを備える物品。

【請求項 4 2】

請求項 4 0 記載のIDタグを備える物品であって、

前記拡張IDは、さらに、拡張IDの桁数、改竄検知符号の桁数と計算方法を示すバージョン情報を含み、前記改竄検知符号は、前記バージョン情報に対する改竄をも検知するものであるIDタグを備える物品。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、IDの管理を行う技術に関し、特に、改竄検知符号を備えたIDの、発

行と流通の管理を行う技術に関する。

【 0 0 0 2 】

【従来の技術】

従来より、JANコードなどの様々なIDが物品に付与され、物品の管理に利用されている。物品に関する情報を、物品に付与したID(物品識別子)と関連付けて管理することにより、物品を個別に管理することができる。

【 0 0 0 3 】

例えば、コンビニエンスストアなどでは、商品の製造会社や名前や価格を、商品の包装に印字されているJANコードと関連付けて管理しておき、バーコードを読み取ることでJANコードを入力すれば商品の情報を参照できるシステムを利用している。

【 0 0 0 4 】

また、値が正しいものであることを保証するため、IDに誤り検知符号を備える。読み取ったIDの誤り検知符号を所定の計算手順により検証することで、読み取りが正常に行われたか否かが判断できる。さらに、鍵となる数値を利用して計算する誤り検知符号には、鍵を知らない者によるIDの改竄を検知する機能がある。以下では、鍵を利用して計算する誤り検知符号のことを改竄検知符号と呼ぶ。

【 0 0 0 5 】

IDに高い安全性が求められる場合、改竄検知符号を備えたIDを利用する。例えば、身分証明証などのようなIDの付与された物品を人と関連付けることにより、人を個別に管理する場合や、株券や商品券などの有価証券にIDを付与して管理する場合などがある。

【 0 0 0 6 】

【発明が解決しようとする課題】

上記従来のIDの管理方法には、以下のような問題がある。

【 0 0 0 7 】

すなわち、上記コンビニエンスストアの例の様にJANコードを物品のIDとして利用する場合、IDの桁数制限により物品の種類別にIDを振り分けているため、同じ種類の物品において、1つ1つ個別に管理することはできない。また、個別管

理ができるようにJANコードよりも桁数を増やしたIDがあるが、バーコードで表示する場合、スペースの都合により適用できない物品もある。

【 0 0 0 8 】

また、JANコードは誤り検知符号しか備えておらず、鍵を用いた改竄検知符号は備えていない。このため、IDを偽造されるおそれがある。偽造防止のため、IDに改竄検知符号を用いる場合は、安全のため、いくつかのID毎に異なる鍵を利用する必要がある。このため、上記コンビニエンスストアの例の様に、様々な種類のIDを扱う場合、扱うID全ての改竄検知符号の検証用の鍵をあらかじめ用意しておかねばならない。

【 0 0 0 9 】

また、改竄検知符号を備えたIDを利用した物品管理を個人が行なう場合、IDが付与されたシールやテープを入手し、任意の物品に貼り付けて管理する方法などが考えられるが、改竄検知符号の検証用の鍵も管理する必要があり、困難である。

【 0 0 1 0 】

また、IDに高い安全性が求められる場合、IDが重複しないように発行の管理を行なうか、もしくは、同一IDの個数の管理を行なう必要がある。このためには、物品やシールへのIDの印字や、電子タグに利用するメモリへの書き込みも、管理しなければならない。

【 0 0 1 1 】

また、IDが重複しないように安全性高く発行の管理を行なっているものとして、クレジットカードのIDが挙げられる。しかし、クレジットカードのIDのように、サービスや、サービスを受ける人・法人に対して与えられているIDは、物品としての実体がなく情報にすぎないため、発行後に不正に複製されてしまう恐れがある。

【 0 0 1 2 】

本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、改竄検知符号を備え、物品個別に割り当て可能なIDの発行と流通を管理し、IDを利用した物品管理を効率よく、かつ、信頼性高く行うことが可能な仕組みを提供すること

にある。

【 0 0 1 3 】

【課題を解決するための手段】

上記目的を達成するために、本発明では、同じ種類の物品であっても異なるIDを個別に割り当て可能であり、さらに属性情報と改竄検知符号を備えた拡張型物品識別子（以下、拡張IDという）を利用する。属性情報とはIDを分類する情報で、IDの利用分野や、発行を依頼した会社名などを表わす情報である。そして、IDの備える改竄検知符号は、属性情報ごとに異なる鍵を用いて生成する。

【 0 0 1 4 】

また、本発明では、IDの発行と流通を管理するためのID管理端末を設け、ネットワークを介して、IDを利用するためのID利用端末に接続する。ID管理端末には、発行したIDと、IDの属性情報と、改竄検知符号と、改竄検知符号の検証用の鍵を、関連付けて格納する。そして、ID管理端末は、IDとIDの属性情報と改竄検知符号とを含む改竄検知符号102の検証要求が、ID利用端末から送られてきた場合、格納しているIDと、それに関連付けられている改竄検知符号とを用いて検証し、結果を端末に返す。以下、検証要求とは、改竄検知符号102の検証要求を指す。また、IDの属性情報を含む検証用鍵要求がID利用端末から送られてきた場合、IDの属性情報と関連づけられている検証用の鍵を、端末に返す。ID利用端末は、IDを読み取る機能と、読み取ったIDとIDが付与されている物品の情報とを関連付けて管理する機能と、物品の情報が処理を示すものであった場合にその処理を行なう機能を有している。

【 0 0 1 5 】

また、本発明では、ID受注端末とIDタグ製造工場用端末を設け、ネットワークを介してID管理端末と接続する。ID受注端末は、IDの発行を依頼された日付け、個数、改竄検知符号の生成用の鍵などを格納し、生成用の鍵を用いて改竄検知符号の生成を行なう。IDと、IDの属性情報と、改竄検知符号をひとつにまとめる。暗号通信を利用してID管理端末に送信し、ID管理センタで管理している情報から、発行済みのIDと重複していないことを確認した後、同様に暗号通信を利用してIDタグ製造工場用端末に送信する。ここで、IDがバーコードと同じ情報を示して

いる旨を属性情報に含ませて、複数個の同一IDを発行してもよい。

【0016】

一方、IDタグ製造工場用端末は、バーコードラベルや電子タグなどのIDタグを製造する製造部に対し、IDと、IDの属性情報と、改竄検知符号を、IDタグ上に印字、もしくは、IDタグ内に格納するよう、指示する。また、IDタグの検査部に対し、完成したIDタグに情報が正しく格納されているかどうかを検査するよう、指示する。そして、製造したIDタグの情報と検査結果を、暗号通信を利用してID管理端末に送信する。

【0017】

本発明によれば、IDを重複すること無く発行し、物品の個別管理を行なうことが可能となる。また、複数個の同一IDを発行し、IDを既存のバーコードシステムで利用することが可能となる。

【0018】

また、本発明によれば、IDの利用者は、検証用の鍵や装置を保持していなくても、ID利用端末からID管理端末に、ネットワークを通じてIDタグから読みとった情報（例えば、IDとIDの属性情報と改竄検知符号）を用いた検証要求を送信すれば、検証結果を得ることができる。

【0019】

また、本発明によれば、IDの利用者は、検証用の鍵を保持していなくても、ID利用端末からID管理端末に、ネットワークを通じてIDの属性情報を含む検証用鍵要求を送信すれば、検証用の鍵を得ることができ、改竄検知符号の検証を行なうことができる。

【0020】

また、本発明によれば、改竄検知符号の生成用および検証用の鍵や、IDの発行依頼者の情報などの、機密性の高い情報を秘密裏に管理することができる。

【0021】

また、本発明において、IDタグとして電子回路チップを用いる場合を考える。電子回路チップを製造するには、十分な設備が必要である。そして、電子回路チップを小型・薄型にするほど、電子回路チップを製造できる者が限られてくる。

このため、不正な第三者がIDタグの複製を製造する可能性が低くなる。また、IDを電子回路チップの書き換え不可領域に格納すれば、不正な第三者がIDを改変することはできない。したがって、本発明によれば、ID管理端末が市場に流通するIDタグの個数を管理することができる。

【 0 0 2 2 】

【発明の実施の形態】

以下、本発明の一実施形態が適用されたID管理システムについて説明する。

【 0 0 2 3 】

まず、本実施形態のID管理システムで用いるIDおよびIDタグについて説明する。

【 0 0 2 4 】

図1は本実施形態のID管理システムで用いるIDの一例を示した図である。

【 0 0 2 5 】

図1(a)に示すように、本実施形態で用いるID100は、IDの属性情報101と、改竄検知符号102を伴ない、拡張ID200として一まとめで利用される。属性情報101とはID100を分類する情報で、ID100の利用分野や、発行を依頼した会社名などを表わす情報である。また、改竄検知符号102は、属性情報101ごとに異なる鍵を用いて、ID100と属性情報101に対して所定の計算を行ない生成される。改竄検知符号102を生成するための計算には、公開鍵暗号、共通鍵暗号、ハッシュ生成関数などを組み合わせたものを利用するとよい。

【 0 0 2 6 】

図1(b)は、図1(a)の3要素にクラス情報103が付随する場合を示している。クラス情報とは、ID100と属性情報101の切り分け位置、すなわち、それぞれの桁数を示す情報である。図1(c)、(d)、(e)に示すように、クラス情報103を用いれば、拡張ID200と改竄検知符号102が同じ桁数でありながら、ID100と属性情報101の桁数や個数を様々に変えた拡張ID200を構築することができる。このため、拡張ID200の受け渡しや、改竄検知符号102の生成および検証に用いる仕組みを変えなく、用途に応じて、ID100と属性

情報 1 0 1 の桁数や個数の組み合わせが最適な拡張 ID 2 0 0 を利用できる。

【 0 0 2 7 】

また、図 1 (f) は、図 1 (a) の 3 要素にバージョン情報 1 0 4 が付随する場合を示している。バージョン情報とは、拡張 ID 2 0 0 のバージョンを示す情報である。バージョン情報 1 0 4 から、拡張 ID 2 0 0 の桁数、改竄検知符号 1 0 2 の桁数と計算方法などが分かる。

【 0 0 2 8 】

また、図 1 (g) は、拡張 ID 2 0 0 が暗号化してある場合を示している。暗号化してあることを示す暗号化符号 1 0 5 と、図 1 (a) の 3 要素を暗号化した情報 1 0 6 からなる。拡張 ID 2 0 0 を暗号化して用いると、復号化用の鍵を知らない者には拡張 ID 2 0 0 の構成要素が判別できないため、不正な解読を防止することができる。

【 0 0 2 9 】

なお、拡張 ID 2 0 0 は上記に限らず、クラス情報 1 0 3 の追加、バージョン情報 1 0 4 の追加、暗号化、のうちの任意の 2 つ、または、全てを組み合わせたものでも良い。

【 0 0 3 0 】

図 2 は本実施形態の ID 管理システムで用いる ID タグの一例を示した図である。

【 0 0 3 1 】

図 2 (a) は、テープ状の ID タグ 3 0 0 に電子回路チップ 3 0 1 が複数個装着されている様子を示す。適切な位置でテープを切断することで、任意の個数の電子回路チップが装着されたテープ片を得ることができる。

【 0 0 3 2 】

なお、ID タグ 3 0 0 は、電子回路チップ 3 0 1 が装着されているテープ状のものとしたが、シート状のものであってもよいし、電子回路チップ 3 0 1 そのものでもよい。また、ID が印刷されたラベルであってもよい。

【 0 0 3 3 】

電子回路チップ 3 0 1 は、たとえば、十分な設備を有する半導体製造メーカーでなければ製造できない 0.3mm 角程度の小型電子回路チップであり、薄型の略直方

体の形状を有している。また、図2(b)に示すように、シリコンチップ302上に、メモリおよびその読み出し回路として機能する電子回路303と、コンデンサ304と、アンテナ305とが、形成されて構成されている。メモリは、書き換え不可能なメモリ部分を含むものとする。また、書き換え不可能なメモリ部分には、拡張ID200が格納されている。

【0034】

なお、電子回路303の書き換え不可能なメモリ部分への拡張ID200の格納は、電子回路チップ301の製造業者が、当該チップ301をIDタグ300の製造業者へ出荷する前に、予め行っておくようにする。電子回路303の書き換え不可能なメモリ部分とは、ROMなどの書き換え不可能なメモリの他、たとえば、拡張ID200が書き込まれた部分が書き換え不可に設定されている、EEPROMなどの書き換え可能なメモリも含むものとする。

【0035】

電子回路303とコンデンサ304とアンテナ305は、図2(c)に示すような回路を形成している。この回路は、外部から与えられた電波により、アンテナ305にて電流を誘起し、電荷をコンデンサ304に蓄積する。そして、コンデンサ304に蓄積した電荷から得た電力を用いて、電子回路303に記憶されている情報を、アンテナ305より電波を用いて送信する。すなわち、この電子回路チップ301に電波を与えることにより、外部より非接触で電子回路チップ301の電子回路303に格納されている拡張ID200を読み出すことができる。

【0036】

次に、以上のようなIDタグ300を利用して拡張ID200の管理を行う、ID管理システムの構成について説明する。

【0037】

図3は、本実施形態が適用されたID管理システムの概略図である。

【0038】

図示するように、本実施形態のID管理システムは、ID受注端末3と、IDタグ製造工場用端末4と、ID管理端末5とが、専用ネットワークやインターネットなどのネットワーク1に接続されて構成される。なお、図3に示す例では、端末3お

よび4をそれぞれ1つ示しているが、複数であってもかまわない。また、顧客端末8は、専用ネットワークやインターネットなどのネットワーク7を介して、ID受注端末3に接続されている。また、ID管理端末5は、専用ネットワークやインターネットなどのネットワーク2を介して、ID利用端末6に接続されている。ネットワーク1とネットワーク2とネットワーク7とは、同じネットワークであってもよい。

【 0 0 3 9 】

顧客端末8は、IDタグ300を発注するために必要な発注情報を、顧客が入力する端末であり、発注情報をID受注端末3に送信する。

【 0 0 4 0 】

ID受注端末3は、拡張ID200の発行を受注するための端末であり、顧客端末8から送られてきた発注情報から、ID100、属性情報101、改竄検知符号102などを含む拡張ID200を生成し、IDタグ製造工場用端末4に送信する。

【 0 0 4 1 】

また、IDタグ製造工場用端末4は、IDタグ300の製造を管理する端末であり、ID受注端末3から送られてきた拡張ID200が付与されたIDタグ300の製造状況をID管理端末5に送信する。

【 0 0 4 2 】

また、ID管理端末5は、ID受注端末3とIDタグ製造工場用端末4から送られてくる情報を管理し、ID利用端末6から送られてくる要求に応える。

【 0 0 4 3 】

また、ID利用端末6は、IDタグ300から拡張ID200を読み取り、拡張ID200と関連付けて管理している情報を利用するための端末であり、必要に応じて、ID管理端末5に要求を送信する。

【 0 0 4 4 】

なお、ID管理端末5に、ID受注端末3としての機能を持たせるようにすることで、ID受注端末3を省略してもよい。また、ID管理端末5に、IDタグ製造工場用端末4としての機能を持たせるようにすることで、IDタグ製造工場用端末4を省略してもよい。また、ID管理端末5に、ID利用端末6としての機能を持たせるよ

うにすることで、ID利用端末6を省略してもよい。また、ID受注端末3に、顧客端末8としての機能を持たせるようにすることで、顧客端末8を省略してもよい。

【0045】

なお、顧客端末8とID利用端末6は複数個あってもよい。

【0046】

なお、顧客端末8とID受注端末3間、および、ID受注端末3とIDタグ製造工場用端末4間、および、ID受注端末3とID管理端末5間、および、IDタグ製造工場用端末4とID管理端末5間、および、ID管理端末5とID利用端末6間の通信には、暗号を用いることが望ましいが、暗号通信の方式は、それぞれ2つの端末間で通信できれば、異なる方式であってもよい。また、暗号通信を行なう代わりに、あらかじめ認証を行なった後で通信を行なってもよい。

【0047】

次に、上記のID管理システムを構成する各装置について説明する。

【0048】

図16は、顧客端末8の機能構成を示す概略図である。

【0049】

図示するように、顧客端末8は、入出力部81と、通信部82を有する。

【0050】

入出力部81は、IDタグ300の発注に必要な発注情報を受け入れる。発注情報とは、IDタグ300に格納したいID100、暗号化した拡張ID200の復号化用の鍵、など拡張ID200の生成と管理に必要な情報と、発注者情報、発注日時、納入期限、納入方法指定、などIDタグ300の発注に必要な情報と、を指す。

【0051】

また、ID受注端末3から受け取った受注情報を出力する。受注情報とは、前記発注情報と、IDタグ300に格納される拡張ID200、ID受注端末3が改竄検知符号を生成するために用いた鍵と、検証するために用いる鍵、自動生成された暗号化用及び復号化用の鍵、など拡張ID200の管理に必要な情報と、受注日時、納入日時、納入方法、などIDタグ300の納入に必要な情報と、を指す。

【 0 0 5 2 】

通信部 8 2 は、入出力部 8 1 より受け取った発注情報を含む受注情報要求を、通信用に暗号化し、ネットワーク 7 を介して ID 受注端末 3 に送信する。また、ID 受注端末 3 より、暗号化された受注情報を受け取り、復号化する。通信用の暗号化には、共通鍵暗号、もしくは、公開鍵暗号、もしくは、共通鍵暗号と公開鍵暗号を組み合わせたもの、を利用する。

【 0 0 5 3 】

図 4 は、ID 受注端末 3 の機能構成を示す概略図である。

【 0 0 5 4 】

図示するように、ID 受注端末 3 は、入出力部 3 1 と、拡張 ID 生成部 3 2 と、改竄検知符号生成部 3 3 と、通信部 3 4 を有する。

【 0 0 5 5 】

通信部 3 4 は、ネットワーク 7 を介して顧客端末 8 より受信した暗号文の復号化を行ない、発注情報を含む受注情報要求を得る。利用する暗号方式は、顧客端末 8 の通信部 8 2 で利用しているものと同じとする。

【 0 0 5 6 】

入出力部 3 1 は、エラー情報などを出力する。また、発注情報をネットワーク 7 を介して顧客端末 8 から受け入れず、直接入力受付する場合に用いる。

【 0 0 5 7 】

拡張 ID 生成部 3 2 は、通信部 3 4 より受け取った発注情報から、ID の属性情報 1 0 1 を生成する。また、改竄検知符号生成部 3 3 に、ID 1 0 0 と属性情報 1 0 1 と改竄検知符号生成用の鍵を渡し、生成された改竄検知符号 1 0 2 と検証用の鍵を受け取る。発注情報に改竄検知符号生成用の鍵が含まれていない場合、乱数を生成し、生成した値を改竄検知符号生成用の鍵とする。さらに、ID 1 0 0 と属性情報 1 0 1 と改竄検知符号 1 0 2 から、拡張 ID 2 0 0 を生成する。なお、属性情報 1 0 1 は、クラス情報 1 0 3 であってもよいし、バージョン情報 1 0 4 であってもよい。また、発注情報に拡張 ID 2 0 0 の暗号化用の鍵が含まれていない場合、乱数を生成し、生成した値を暗号化用の鍵とする。また、拡張 ID 2 0 0 を暗号化し、暗号化符号 1 0 5 を生成し、復号化用の鍵を生成する機能も有する。発

注情報に、拡張ID、生成した鍵などを加え、受注情報とする。

【0058】

改竄検知符号生成部33は、拡張ID生成部32より受け取ったID100と属性情報101と改竄検知符号生成用の鍵から、改竄検知符号102と検証用の鍵とを生成し、拡張ID生成部32に渡す。

【0059】

通信部34は、ネットワーク7を介して顧客端末8より受け取った発注情報を含むID重複確認要求を、通信用に暗号化し、ネットワーク1を介してID管理端末5に送信する。なお、発注情報の代わりに入出力部31より受け取った拡張ID200を送信してもよい。ID管理端末5より、発行済みIDとの重複がない旨の通知を受け取った後、入出力部31より受け取った受注情報を含む受注ID登録要求を通信用に暗号化し、ネットワーク1を介してID管理端末5に送信する。なお、IDの重複を許可する場合は、ID重複確認要求の送信を省略しても良い。

【0060】

また、入出力部31より受け取った受注情報を含むIDタグ製造要求を通信用に暗号化し、ネットワーク1を介してIDタグ製造工場用端末4に送信する。通信用の暗号化には、共通鍵暗号、もしくは、公開鍵暗号、もしくは、共通鍵暗号と公開鍵暗号を組み合わせたもの、を利用する。また、入出力部31より受け取った受注情報を通信用に暗号化し、ネットワーク7を介して顧客端末8に送信する。利用する暗号方式は、顧客端末8の通信部82で利用しているものと同じとする。

【0061】

図5は、IDタグ製造工場46の機能構成を示す概略図である。

【0062】

図示するように、IDタグ製造工場46は、IDタグ製造工場用端末4と、製造部42と、検査部43と、納入部45とを有する。また、IDタグ製造工場用端末4は、通信部41と、制御部44とを有する。

【0063】

通信部41は、ネットワーク1を介してID受注端末3より受信した暗号文の復

号化を行ない、受注情報を含むIDタグ製造要求を得る。利用する暗号方式は、ID受注端末3の通信部34で利用しているものと同じとする。

【0064】

制御部44は、通信部41で得た受注情報を受け取り、該受注情報に含まれる拡張ID200を格納したIDタグ300を、該受注情報に従って製造するよう、製造部42に指示する。また、拡張ID200を検査部43に送り、完成したIDタグ300の機能が正常か否かを検査するよう、検査部43に指示する。検査結果が不良であった場合、拡張ID200を製造部42に渡し、再度、IDタグ300を製造させる。検査結果が不良であった拡張ID200を、欠番IDとして通信部41に渡してもよい。また、検査結果が正常であったIDタグ300に付与されている拡張ID200を製造済みIDとして通信部41に渡す。

【0065】

通信部41は、欠番IDを含む欠番ID登録要求と、製造済みIDを含む製造済みID登録要求と、を作成し、通信用に暗号化し、ネットワーク1を介してID管理端末5に送信する。通信用の暗号化には、共通鍵暗号、もしくは、公開鍵暗号、もしくは、共通鍵暗号と公開鍵暗号を組み合わせたもの、を利用する。

【0066】

製造部42は、制御部44より受け取った拡張ID200を格納したIDタグ300を製造する。そして、製造したIDタグ300を検査部43に渡す。

【0067】

検査部43は、製造部42から受け取ったIDタグ300を検査し、制御部44より受け取った拡張ID200が正しく格納されていることなどを確認する。そして、検査結果を制御部44に送る。

【0068】

納入部45は、検査部43で検査結果が合格であったIDタグ300を受け取る。そして、受注情報に含まれる納入方法に従って、顧客に対して発送・引き渡しなどを行ない、納入する。

【0069】

図6は、ID管理端末5の機能構成を示す概略図である。

【 0 0 7 0 】

図示するように、ID管理端末 5 は、通信部 5 1 と、ID関連情報管理部 5 2 と、ID関連情報管理データベース 5 3 とを有する。

【 0 0 7 1 】

通信部 5 1 は、ネットワーク 1 を介してID受注端末 3 より受信した暗号文の復号化を行ない、受注情報を含むID重複確認要求、もしくは、受注情報を含む受注ID登録要求を得る。利用する暗号方式は、ID受注端末 3 の通信部 3 4 で利用しているものと同じとする。また、ネットワーク 1 を介してIDタグ製造工場用端末 4 より受信した暗号文の復号化を行ない、欠番IDを含む欠番ID登録要求と、製造済みIDを含む製造済みID登録要求と、を得る。利用する暗号方式は、IDタグ製造工場用端末 4 の通信部 4 1 で利用しているものと同じとする。また、ネットワーク 2 を介してID利用端末 6 より受信した暗号文の復号化を行ない、拡張ID 2 0 0 を含む検証要求、もしくは、属性情報 1 0 1 を含む検証用鍵要求、もしくは、復号化用鍵要求を得る。利用する暗号方式は、ID利用端末 6 の通信部 6 1 で利用しているものと同じとする。

【 0 0 7 2 】

ID関連情報管理部 5 2 は、通信部 5 1 より受け取った要求が、ID重複確認要求である場合、共に受け取った受注情報に含まれる拡張ID 2 0 0 と、ID関連情報管理データベース 5 3 に格納してある拡張ID 2 0 0 とを用いて、発行済みIDと重複するか否かを確認する。そして、確認の結果を通信部 5 1 で暗号化し、ネットワーク 1 を介してID受注端末 3 に送信する。また、通信部 5 1 より受け取った要求が、受注ID登録要求である場合、共に受け取った受注情報をID関連情報管理データベース 5 3 に格納する。また、通信部 5 1 より受け取った要求が、欠番ID登録要求である場合、共に受け取った欠番IDをID関連情報管理データベース 5 3 に格納する。また、通信部 5 1 より受け取った要求が、製造済みID登録要求である場合、共に受け取った製造済みIDをID関連情報管理データベース 5 3 に格納する。また、通信部 5 1 より受け取った要求が、検証要求である場合、共に受け取った拡張ID 2 0 0 と、ID関連情報管理データベース 5 3 に格納してある拡張ID 2 0 0 とを比較し、検証を行なう。そして、検証結果を通信部 5 1 で暗号化し、ネット

ワーク 2 を介して ID 利用端末 6 に送信する。また、通信部 5 1 より受け取った要求が、検証用鍵要求である場合、共に受け取った属性情報 1 0 1 から、ID 関連情報管理データベース 5 3 に格納してある改竄検知符号 1 0 2 の検証用の鍵を取り出し、通信部 5 1 で暗号化し、ネットワーク 2 を介して ID 利用端末 6 に送信する。また、通信部 5 1 より受け取った要求が、復号化用鍵要求である場合、ID 関連情報管理データベース 5 3 より復号化用の鍵を取り出し、通信部 5 1 で暗号化し、ネットワーク 2 を介して ID 利用端末 6 に送信する。通信用の暗号化には、共通鍵暗号、もしくは、公開鍵暗号、もしくは、共通鍵暗号と公開鍵暗号を組み合わせたもの、を利用する。また、通信部 5 1 より受け取った要求が、失効 ID 登録要求である場合、共に受け取った失効 ID 2 0 0 を、ID 関連情報管理データベース 5 3 に格納する。

【 0 0 7 3 】

ID 関連情報管理データベース 5 3 には、ID タグ 3 0 0 に関連する管理情報が格納される。図 1 7 は、ID 関連情報管理データベース 5 3 に格納される ID タグ 3 0 0 に関連する管理情報を説明するための図である。図示するように、ID タグ 3 0 0 に関連する管理情報は、ID 受注端末 3 から送られてきた受注情報 5 3 0 と、発行/納入済み・欠番扱い・製造中・失効などの ID の発行状況 5 3 8 と、その他の管理情報である備考 5 3 9 と、を含んで構成される。

【 0 0 7 4 】

ここで、受注情報 5 3 0 は、顧客端末 8 において受け入れた発注情報 5 3 1 と、ID 受注端末 3 において前記発注情報 5 3 1 から生成された拡張 ID 2 0 0 と、を含む。ここで、発注情報 5 3 1 は、顧客情報 5 3 2 と、顧客が発注した ID の個数 5 3 3 と、欠番や重複などの発行条件 5 3 4 と、ID 3 0 0 の指定納入日 5 3 5 と、ID の属性情報 1 0 1 と対応づけられた改竄検知コード 1 0 2 の検証用の鍵 5 3 6 と、拡張 ID 2 0 0 が暗号化されて ID タグ 3 0 0 に付与されている場合の復号化用の鍵 5 3 7 と、顧客が発行を希望した ID 1 0 0 と、を含んで構成される。

【 0 0 7 5 】

図 7 は、ID 利用端末 6 の機能構成を示す概略図である。図示するように、ID 利用端末 6 は、ID 読み取り部 6 1 と、入出力部 6 2 と、制御部 6 3 と、データベー

ス 6 4 と、通信部 6 5 とを有する。

【 0 0 7 6 】

ID読み取り部 6 1 は、IDタグ 3 0 0 に付与された拡張ID 2 0 0 を読み取る。たとえば、拡張IDが電子回路チップ 3 0 1 のメモリに格納されている場合、電波を送信してIDタグ 3 0 0 に装着された電子回路チップ 3 0 1 を駆動する。そして、当該電子回路チップ 3 0 1 から送信されるデータを読み取る。受信したデータに暗号化符号 1 0 5 がある場合は、受信したデータを復号化し、拡張ID 2 0 0 を得る。復号化に用いる鍵は、あらかじめデータベース 6 4 に格納しておいてもよいし、通信部 6 5 を通じてID管理端末 5 に復号化用鍵要求を送信してID管理端末 5 から入手してもよい。また、読み取った拡張ID 2 0 0 を含む検証要求を通信部 6 5 を通じてID管理端末 5 に送信し、ID管理端末 5 から検証結果を入手してもよい。

【 0 0 7 7 】

入出力部 6 2 は、データベース 6 4 に対し、新規に登録する情報、または、更新する情報の入力、及び、読み出した情報の表示を行なう。また、IDの読み取り、データベースの読み書き、通信、などの指示を受け入れ、結果を出力する。

【 0 0 7 8 】

制御部 6 3 は、ID読み取り部 6 1 と、入出力部 6 2 と、データベース 6 4 と、通信部 6 5 とを制御する。また、読み取った拡張ID 2 0 0 の改竄検知符号 1 0 2 の検証を行なう。検証用の鍵は、データベース 6 4 に格納しておいてもよいし、属性情報 1 0 1 を含む検証用鍵要求をID管理端末 5 に対して送信して、ID管理端末 5 から入手してもよい。改竄検知符号 1 0 2 の検証は、拡張ID 2 0 0 を含む検証要求をID管理端末 5 に送信して、検証結果をID管理端末 5 から入手してもよい。改竄検知符号 1 0 2 の検証に成功したならば、対応づけて格納してある情報をデータベース 6 4 から取り出し、入出力部 6 2 で出力する。なお、取り出した情報が処理を示すものである場合、当該処理を行なう。当該処理には、たとえば、決済処理、他の端末への転送、情報が示すURLに対する問い合わせ、などがある。IDの読み取りに失敗した場合は、ID読み取り部 6 1 に再度読み取り作業を行なわせるか、または、当該IDを失効IDとし、電子署名を付加し、通信部 6 5 に失効

ID登録要求をID管理端末5に送信させる。

【0079】

データベース64は、拡張ID200と、拡張ID200が付与されたIDタグ300と対応づけられて管理されている物品の情報とを格納する。また、IDの属性情報101と、対応する改竄検知符号102の検証用の鍵とを、関連付けて格納する。また、IDタグ300に付与された暗号化した拡張ID200を復号化するための鍵を格納する。

【0080】

通信部65は、復号化用鍵要求と、属性情報101を含む検証用鍵要求と、拡張ID200を含む検証要求と、失効IDを含む失効ID登録要求と、を作成し、通信用に暗号化し、ネットワーク2を介してID管理端末5に送信する。通信用の暗号化には、共通鍵暗号、もしくは、公開鍵暗号、もしくは、共通鍵暗号と公開鍵暗号を組み合わせたもの、を利用する。

【0081】

なお、ID読み取り部61と入出力部62は、ID利用端末6以外の他の端末のものを利用し、ID利用端末6とネットワークを介して接続してもよい。また、ID読み取り部61と入出力62は、それぞれ複数個あってもよい。

【0082】

なお、上記の顧客端末8、ID受注端末3、IDタグ製造工場用端末4、およびID管理端末5は、図8に示すように、CPU71と、メモリ72と、ハードディスク装置などの外部記憶装置73と、FD、CD-ROM、DVD-ROMなどの記憶媒体74からデータを読み取る記憶媒体読取装置75と、キーボード、マウスなどの入力装置76と、モニタなどの出力装置77と、ネットワークを介して他の装置と通信を行うための通信装置78と、これら装置間のデータ送受を司るインターフェース79と、を備えた一般的な構成を有する電子計算機上に、構築することができる。

【0083】

上記のID受注端末3の入出力部31、拡張ID生成部32、改竄検知符号生成部33、通信部34、ID管理端末5の通信部51、ID関連情報管理部52およびID

関連情報管理データベース 53 は、CPU 71 がメモリ 72 上にロードされたプログラムを実行することで、電子計算機上に具現化されるプロセスとして実現される。また、ID管理端末 5 の場合、メモリ 72 や外部記憶装置 73 がID関連情報管理データベース 53 として使用される。

【 0 0 8 4 】

この、CPU 71 により実行されることで電子計算機上に上記のID受注端末 3 を具現化するためのプログラムは、予め外部記憶装置 73 に記憶され、必要に応じてメモリ 72 上にロードされ、CPU 71 により実行される。あるいは、記憶媒体読取装置 75 を介して記憶媒体 74 からメモリ 72 上にロードされ、CPU 71 により実行される。もしくは、一旦、記憶媒体読取装置 75 を介して記憶媒体 74 から外部記憶装置 73 にインストールされた後、必要に応じて、外部記憶装置 73 からメモリ 72 上にロードされ、CPU 71 により実行される。さらには、他の計算機から、ネットワーク上の伝送媒体と通信装置 78 を介して、いったん外部記憶装置 73 にダウンロードされ、それからメモリ 72 上にロードされ、あるいは直接ネットワークからメモリ 72 上にロードされて、CPU 71 により実行される。

【 0 0 8 5 】

また、上記のID利用端末 6 は、図 8 に示す電子計算機、および、電子回路チップ読取装置、バーコード読取装置、OCR、電子スキャナなどのID読取装置 710 を有するシステム上に、構築することができる。上記のID利用端末 6 のID読み取り部 61、入出力部 62、制御部 63、データベース 64 および通信部 65 は、CPU 71 がメモリ 72 上にロードされたプログラムを実行することで、システム上に具現化されるプロセスとして実現される。また、この場合、メモリ 72 や外部記憶装置 73 がデータベース 64 として使用される。この、CPU 71 により実行されることでシステム上に上記のIDタグ製造工場用端末 4 を具現化するためのプログラムは、予め外部記憶装置 73 に記憶され、必要に応じてメモリ 72 上にロードされ、CPU 71 により実行される。あるいは、記憶媒体読取装置 75 を介して記憶媒体 74 からメモリ 72 上にロードされ、CPU 71 により実行される。もしくは、一旦、記憶媒体読取装置 75 を介して記憶媒体 74 から外部記憶装置

73にインストールされた後、必要に応じて、外部記憶装置73からメモリ72上にロードされ、CPU71により実行される。さらには、他の計算機から、ネットワーク上の伝送媒体と通信装置78を介して、いったん外部記憶装置73にダウンロードされ、それからメモリ72上にロードされ、あるいは直接ネットワークからメモリ72上にロードされて、CPU71により実行される。

【0086】

次に、上記のID管理システムの動作について説明する。

【0087】

まず、顧客端末8の動作について説明する。

【0088】

図18は、顧客端末8の動作の概略を説明するためのフロー図である。

【0089】

まず、入出力部81において、IDタグ300の発注情報を受け入れる（ステップ1801（S1801という、以下同様））。

【0090】

次に、通信部82は、S1801で受け入れた発注情報を含む、受注情報要求を作成し、通信用に暗号化してネットワーク7を介してID受注端末3に送信する（S1802）。そして、ID受注端末3から、受注情報を受信するまで待機する（S1803）。受信したならば（S1803のYes）、通信部82は受信した暗号文の復号化を行ない、入出力部81は、通信部82で得た受注情報を出力する（S1804）。

【0091】

次に、ID受注端末3の動作について説明する。

【0092】

図9は、ID受注端末3の動作の概略を説明するためのフロー図である。

【0093】

まず、通信部41は、ネットワーク7を介して顧客端末8から発注情報を含む受注情報要求を受信するまで、待機する（S1316）。受信したならば（S1316のYes）、通信部41は、受信した暗号文の復号化を行ない、発注情報

を入手する（S 1 3 0 1）。

【 0 0 9 4 】

次に、通信部 3 4 は、S 1 3 0 1 で受け入れた発注情報を含む、ID重複確認要求を作成し、通信用に暗号化してネットワーク 1 を介してID管理端末 5 に送信する（S 1 3 0 2）。そして、ID管理端末 5 から、前記ID重複確認要求に対する処理結果を受信するまで待機する（S 1 3 0 3）。

【 0 0 9 5 】

次に、発注情報が示すIDとID管理端末 5 に登録済みのIDとが重複していた場合（S 1 3 0 4 の Y e s）、入出力部 3 1 は、エラーを出力する（S 1 3 0 5）。重複していない場合（S 1 3 0 4 の N o）、拡張ID生成部 3 2 は、発注情報からIDの属性情報 1 0 1、クラス情報 1 0 3、バージョン情報 1 0 4 を生成する（S 1 3 0 6）。発注情報に、改竄検知符号 1 0 2 生成用の鍵、または拡張 I D 2 0 0 の暗号化用の鍵、のいずれかが含まれていない場合（S 1 3 0 7 の N o）は、拡張ID生成部 3 2 は、乱数を生成する（S 1 3 0 8）。

【 0 0 9 6 】

次に、改竄検知符号生成部 3 3 は、発注情報に含まれる改竄検知符号 1 0 2 生成用の鍵と、ID 1 0 0 と、S 1 3 0 6 で生成された属性情報 1 0 1、クラス情報 1 0 3 またはバージョン情報 1 0 4 と、を用いて改竄検知符号 1 0 2 と、検証用の鍵と、を生成する（S 1 3 0 9）。発注情報に、改竄検知符号 1 0 2 生成用の鍵が含まれていない場合は、改竄検知符号 1 0 2 生成用の鍵として、S 1 3 0 8 で入手した乱数値を用いる。

【 0 0 9 7 】

次に、拡張ID生成部 3 2 は、発注情報に含まれるID 1 0 0 と、S 1 3 0 6 で生成された属性情報 1 0 1、クラス情報 1 0 3 またはバージョン情報 1 0 4 と、S 1 3 0 9 で生成された改竄検知符号 1 0 2 と、を用いて拡張ID 2 0 0 を生成する（S 1 3 1 0）。拡張ID 2 0 0 の暗号化が必要であった場合（S 1 3 1 1 の Y e s）は、拡張ID生成部 3 2 は、発注情報に含まれる暗号化用の鍵を用いて暗号化を行ない（S 1 3 1 2）、暗号化符号 1 0 5 を添付する（S 1 3 1 3）。発注情報に、暗号化用の鍵が含まれていない場合は、暗号化用の鍵として、S 1 3 0 8

で入手した乱数値を用いる。

【0098】

次に、通信部34は、S1301で受け入れた発注情報と、S1310で作成した拡張ID200、もしくは、S1313で作成した暗号化した拡張ID200と、S1308で生成した乱数値から得た鍵と、を含む受注情報を生成する（S1317）。

【0099】

次に、通信部34は、S1317で生成した受注情報を含む、受注ID登録要求を作成し、通信用に暗号化してネットワーク1を介してID管理端末5に送信する（S1314）。また、通信部34は、S1317で生成した受注情報を含む、IDタグ製造要求を作成し、通信用に暗号化してネットワーク1を介してIDタグ製造工場用端末4に送信する（S1315）。また、通信部34は、S1317で生成した受注情報を、通信用に暗号化してネットワーク7を介して顧客端末8に送信する（S1318）。

【0100】

なお、S1314、S1315、およびS1318の順番は入れ替わってもよい。

【0101】

なお、S1306～S1310の処理を、S1301の直後に行なってもよい。この場合は、S1302において作成するID重複確認要求には、S1310で生成された拡張ID200が含まれる。

【0102】

次に、IDタグ製造工場用端末4の動作について説明する。

【0103】

図10は、IDタグ製造工場用端末4の動作を説明するためのフロー図である。

【0104】

まず、通信部41は、ネットワーク1を介してID受注端末3からIDタグ製造要求を受信するまで、待機する（S1401）。受信したならば（S1401のYes）、通信部41は、受信した暗号文の復号化を行ない、受注情報を入手する

(S1402)。

【0105】

次に、制御部44は、S1402で入手した受注情報に含まれる拡張ID200を格納したIDタグ300を製造するよう、製造部42に指示し、製造部42は、該受注情報に従ってIDタグ300を製造する(S1403)。

【0106】

次に、制御部44は、S1403で製造されたIDタグ300の機能が正常か否かを検査するよう、検査部43に指示し、検査部43は、製造部42から受け取ったIDタグ300を検査し、制御部44より受け取った拡張ID200が正しく格納されていることなどを確認する。(S1404)。

【0107】

制御部44は、検査部43から受け取った検査結果が正常であったならば(S1405のYes)、IDタグ300に付与されている拡張ID200を、製造済みIDとする(S1406)。通信部41は、S1406で得た製造済みIDを含む、製造済みID登録要求を作成し、通信用に暗号化してネットワーク1を介してID管理端末5に送信する(S1407)。

【0108】

次に、納入部45は、検査部43で検査結果が合格であったIDタグ300を受け取り、受注情報に含まれる納入方法に従って、顧客に対して発送・引き渡しなどを行ない、納入する(S1411)。

【0109】

一方、検査部43から受け取った検査結果が異常であったならば(S1405のNo)、制御部44は、IDタグ300に付与されている拡張ID200を、欠番IDとする(S1408)。検査結果が異常であったIDタグ300の再製造が必要な場合(S1409のYes)、制御部44は、製造部42にIDタグ300の再製造を行なわせ、S1408で得た欠番IDを付与する(S1403)。一方、再製造が必要ない場合(S1409のNo)、通信部41は、欠番IDを含む欠番ID登録要求を作成し、通信用に暗号化してネットワーク1を介してID管理端末5に送信する(S1410)。

【0 1 1 0】

次に、ID管理端末5の動作について説明する。

【0 1 1 1】

図11は、ID管理端末5の動作を説明するためのフロー図である。

【0 1 1 2】

まず、通信部51は、ID受注端末3またはIDタグ製造工場用端末4からネットワーク1を介した要求、もしくは、ID利用端末6からネットワーク2を介した要求、を受信するまで、待機する（S1501）。受信したならば（S1501のYes）、通信部51は、受信した暗号文の復号化を行ない、後述する各種情報を含んだ要求を得る（S1502）。

【0 1 1 3】

次に、ID関連情報管理部52は、S1502で入手した要求内容を解析する。

【0 1 1 4】

入手した要求内容が、ID受注端末3からのID重複確認要求であるならば、ID関連情報管理部52は、前記ID重複確認要求に含まれる発注情報を入手する（S1511）。次に、S1511で入手した発注情報に含まれる拡張ID200と、ID関連情報管理データベース53に格納してある拡張ID200と、を用いて、IDが重複するか否かを確認する（S1512）。ID関連情報管理データベース53に同一の拡張ID200が格納されていても、該拡張ID200が失効扱いであるならば、重複していないものとする。そして、確認の結果を通信部51で暗号化し、ネットワーク1を介してID受注端末3に送信する（S1513）。

【0 1 1 5】

入手した要求内容が、ID受注端末3からの受注ID登録要求であるならば、ID関連情報管理部52は、前記受注ID登録要求に含まれる、受注情報を入手する（S1521）。次に、S1521で入手した受注情報を、ID関連情報管理データベース53に格納する（S1522）。

【0 1 1 6】

入手した要求内容が、IDタグ製造工場用端末4からの製造済みID登録要求であるならば、ID関連情報管理部52は、前記製造済みID登録要求に含まれる製造済

みIDを入手する（S 1 5 3 1）。次に、S 1 5 3 1で入手した製造済みIDを、ID関連情報管理データベース53に格納する（S 1 5 3 2）。

【0 1 1 7】

入手した要求内容が、IDタグ製造工場用端末4からの欠番ID登録要求であるならば、ID関連情報管理部52は、前記欠番ID登録要求に含まれる欠番IDを入手する（S 1 5 4 1）。次に、S 1 5 4 1で入手した欠番IDを、ID関連情報管理データベース53に格納する（S 1 5 4 2）。

【0 1 1 8】

入手した要求内容が、ID利用端末6からの検証要求であるならば、ID関連情報管理部52は、検証要求に含まれる拡張ID200を入手する（S 1 5 5 1）。次に、S 1 5 5 1で入手した拡張ID200と、ID関連情報管理データベース53に格納してある拡張ID200と、を比較して、改竄検知符号102が正当なものであるか否かを検証する（S 1 5 5 2）。そして、検証の結果を通信部51で暗号化し、ネットワーク2を介してID利用端末6に送信する（S 1 5 5 3）。

【0 1 1 9】

入手した要求内容が、ID利用端末6からの検証用鍵要求であるならば、ID関連情報管理部52は、前記改竄検知符号102の検証用鍵要求に含まれる属性情報101を入手する（S 1 5 6 1）。次に、S 1 5 6 1で入手した属性情報101と関連付けられてID関連情報管理データベース53に格納してある、改竄検知符号102の検証用の鍵を取り出す（S 1 5 6 2）。そして、S 1 5 6 2で取り出した改竄検知符号102の検証用の鍵を通信部51で暗号化し、ネットワーク2を介してID利用端末6に送信する（S 1 5 6 3）。

【0 1 2 0】

入手した要求内容が、ID利用端末6からの復号化用鍵要求であるならば、ID関連情報管理部52は、ID関連情報管理データベース53に格納してある、暗号化拡張ID200の復号化用の鍵を取り出す（S 1 5 7 1）。次に、S 1 5 7 1で取り出した暗号化拡張ID200の復号化用の鍵を、通信部51で暗号化し、ネットワーク2を介してID利用端末6に送信する（S 1 5 7 2）。

【0121】

入手した要求内容が、ID利用端末6からの失効ID登録要求であるならば、ID関連情報管理部52は、前記失効ID登録要求に含まれる、失効IDと電子署名を入手する（S1581）。次に、S1581で入手した電子署名により正当な失効ID登録要求であることを確認し、S1581で入手した失効IDを、ID関連情報管理データベース53に格納する（S1582）。

【0122】

次に、ID利用端末6の動作について説明する。

【0123】

図12は、ID利用端末6の動作の概略を説明するためのフロー図である。

【0124】

まず、入出力部62において、指示入力を受け入れる（S1601）。

【0125】

次に、制御部63は、S1601で受け入れた指示の解析を行なう（S1602）。

【0126】

S1601で受け入れた指示が、情報の読み取り指示、または、情報の更新指示、または、情報の新規登録指示の場合、読み取り部61、制御部63、データベース64および通信部65は、ID読取手続（S1603）を行なう。S1603についての詳細は図13～15で説明する。

【0127】

S1601で受け入れた指示が、失効登録指示の場合、制御部63、データベース64および通信部65は、読み取ろうとしたIDタグ300に付与されている拡張ID200を失効扱いとするための失効手続（S1604）を行なう。S1604についての詳細は図19で説明する。

【0128】

S1601で受け入れた指示が、情報の読み取り指示の場合、S1603の後、制御部63は、データベース64より、S1603で入手した拡張ID200と対応づけられて格納されている情報を取り出す（S1605）。そして、S16

05で取り出した情報を入出力部62で出力する、情報の指示に従い決済処理を行なう、情報が示す端末へ転送処理を行なう、など、情報に応じた処理を行なう(S1606)。

【0129】

S1601で受け入れた指示が、更新情報を含む、情報の更新指示の場合、S1603の後、制御部63は、更新情報を入手する(S1607)。そして、データベース64に、S1603で入手した拡張ID200と対応づけられて格納されている情報を、S1607で入手した更新情報で更新する(S1608)。

【0130】

S1601で受け入れた指示が、対応情報を含む、情報の新規登録指示の場合、S1603の後、制御部63は、対応情報を入手する(S1609)。そして、S1609で入手した対応情報と、S1603で入手した拡張ID200と、を対応づけて、データベース64に格納する(S1610)。

【0131】

図13は、図12に示すS1603(ID読取手続)の処理の概要を説明するためのフロー図である。

【0132】

まず、ID読み取り部61は、電波を送信してIDタグ300に装着された電子回路チップ301を駆動する。そして、当該電子回路チップ301から送信されるデータを読み取る(S1611)。

【0133】

次に、制御部63は、S1611で読み取ったデータに暗号化符号105がある場合(S1612のYes)、復号化手続を行なう(S1613)。なお、S1613についての詳細は図14で説明するため、ここでは省略する。

【0134】

次に、制御部63は、S1611で読み取ったデータ、もしくは、S1613で復号化を行なって入手したデータ、の検証手続を行なう(S1614)。なお、S1614についての詳細は図15で説明するため、ここでは省略する。

【0135】

S1614の結果がエラーの場合（S1615のYes）、制御部63は、再読み取りの規定回数内か否かを判断する。（S1618）。規定回数内の場合（S1618のYes）は、再度、IDの読み取りを行なう（S1611）。読み取り回数が規定回数に達している場合（S1618のNo）、入出力部62にエラーを出力する（S1616）。

【0136】

一方、S1614の結果がエラーでない場合（S1615のNo）、制御部63は、正当に検証された拡張ID200を入手する（S1617）。

【0137】

図14は、図13に示すS1613（復号化手続）の処理を説明するためのフロー図である。

【0138】

まず、制御部63は、データベース64に、復号化用の鍵が格納されているか否かを確認する（S1621）。格納されていない場合（S1621のNo）は、通信部65は、復号化用鍵要求を作成し、通信用に暗号化してネットワーク2を介してID管理端末5に送信する（S1622）。そして、ID管理端末5から復号化用の鍵を受信するまで待機する（S1623）。

【0139】

次に、制御部63は、データベース64に格納されている復号化用の鍵、もしくは、S1623で得た復号化用の鍵、を用いて、暗号化拡張ID200を復号化する（S1624）。

【0140】

図15は、図13に示すS1614（検証手続）の処理を説明するためのフロー図である。

【0141】

図13に示すS1614（検証手続）の処理の一例として、まず、図15(a)を説明する。

【 0 1 4 2 】

まず、制御部 6 3 は、データベース 6 4 に、検証用の鍵が格納されているか否かを確認する（S 1 6 3 1）。格納されていない場合（S 1 6 3 1 の N o）は、通信部 6 5 は、属性情報 1 0 1 を含む検証用鍵要求を作成し、通信用に暗号化してネットワーク 2 を介して ID 管理端末 5 に送信する（S 1 6 3 2）。そして、ID 管理端末 5 から検証用の鍵を受信するまで待機する（S 1 6 3 3）。

【 0 1 4 3 】

次に、制御部 6 3 は、データベース 6 4 に格納されている検証用の鍵、もしくは、S 1 6 3 3 で得た検証用の鍵、を用いて、改竄検知符号 1 0 2 の検証を行なう（S 1 6 3 4）。

【 0 1 4 4 】

図 1 3 に示す S 1 6 1 4（検証手続）の処理のもう一つの例として、図 1 5 (b) を説明する。

【 0 1 4 5 】

通信部 6 5 は、拡張 ID 2 0 0 を含む検証要求を作成し、通信用に暗号化してネットワーク 2 を介して ID 管理端末 5 に送信する（S 1 6 3 5）。そして、ID 管理端末 5 から検証結果を受信するまで待機する（S 1 6 3 6）。

【 0 1 4 6 】

図 1 9 は、図 1 2 に示す S 1 6 0 4（失効手続）の処理を説明するためのフロー図である。

【 0 1 4 7 】

まず、入出力部 6 2 において、読み取りに失敗した ID タグ 3 0 0 に関して、該 ID タグ 3 0 0 の表面に印字されている記号や、該 ID タグ 3 0 0 が付与されていた物品の情報、など、該 ID タグ 3 0 0 に付与されている拡張 ID 2 0 0 を推定するためのタグ情報の入力を得る（S 1 6 4 1）。

【 0 1 4 8 】

次に、制御部 6 3 は、S 1 6 4 1 で受け入れたタグ情報をデータベース 6 4 で検索し、対応づけられている拡張 ID 2 0 0 を取り出す（S 1 6 4 2）。取り出した拡張 ID 2 0 0 を失効 ID とする（S 1 6 4 3）。

【 0 1 4 9 】

次に、通信部 6 5 は、電子署名を生成する（S 1 6 4 4）。該電子署名と失効 I D とを含む、失効 I D 登録要求を作成し、通信用に暗号化してネットワーク 2 を介して I D 管理端末 5 に送信する（S 1 6 4 5）。

【 0 1 5 0 】

以上、本発明の一実施形態について説明した。

【 0 1 5 1 】

本実施形態によれば、I D 受注端末 3 と、I D 製造工場用端末 4 および I D 管理端末 5 は、ネットワーク 1 を介して暗号通信を行なっている。また、受注情報、発行済み I D、欠番 I D などの情報を I D 管理端末 5 において一括管理している。また、I D タグ 3 0 0 として、拡張 I D 2 0 0 が書き換え不可領域に格納された電子回路チップ 3 0 1 を利用しているため、不正な第三者が、I D タグ 3 0 0 に付与されている拡張 I D 2 0 0 を改変することはできない。また、電子回路チップ 3 0 1 を製造するには、十分な設備が必要である。そして、電子回路チップ 3 0 1 を小型・薄型にするほど、電子回路チップ 3 0 1 を製造できる者が限られてくるため、不正な第三者が I D タグの複製を製造する可能性が低くなる。また、I D を失効扱いとする際には、その旨を要求してきた I D 利用端末 6 の電子署名を確認し、正当な権利を有する場合のみ、I D を失効扱いとする。以上のことより、I D 管理端末 5 が市場に流通する I D タグ 3 0 0 の個数を管理することができる。また、機密性の高い情報を秘密裏に管理することができる。

【 0 1 5 2 】

また、本実施形態では、I D 利用端末 6 に、検証用の鍵や装置を保持していなくても、I D 管理端末 5 に、ネットワーク 2 を通じて I D 1 0 0 と I D の属性情報 1 0 1 と改竄検知符号 1 0 2 とを含む検証要求を送信すれば、検証結果を得ることができる。

【 0 1 5 3 】

また、本実施形態では、I D 利用端末 6 に、検証用の鍵を保持していなくても、I D 管理端末 5 に、ネットワーク 2 を通じて I D の属性情報 1 0 1 を含む検証用鍵要求を送信すれば、検証用の鍵を得ることができる。

【 0 1 5 4 】

なお、本発明は、上記の実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

【 0 1 5 5 】

たとえば、上記の実施形態において、ID利用端末6は、必ずしも1つの装置上に構築されているものである必要はない。たとえば、拡張ID200の読み取りや、情報または指示の入出力に係わる部分と、データベース64に係わる部分とを、それぞれ別個の装置上に構築し、これらの装置をネットワークで接続するような構成としてもよい。また、それとは逆に、ID利用端末6のデータベース64に係わる部分の機能をID管理端末5に持たせてもかまわない。

【 0 1 5 6 】

また、たとえば、上記の実施形態において、顧客端末8からID受注端末3に送られてくる受注情報要求に含まれる発注情報に、検証用鍵または暗号用鍵が含まれていない場合、ID受注端末3で乱数を生成し、該乱数を鍵として扱うことにしているが、乱数生成機能を顧客端末8に持たせてもよい。この場合、顧客端末8において、生成した乱数を検証用鍵または暗号用鍵として発注情報に含ませ、ID受注端末3に送る。

【 0 1 5 7 】

【発明の効果】

以上説明したように、本発明によれば、改竄検知符号を備えたIDの発行と流通を管理し、IDを利用した物品管理を効率よく、かつ、信頼性高く行うことが可能な仕組みを提供できる。

【図面の簡単な説明】

【図1】

本実施形態のID管理システムで用いるIDの一例を示した図である。

【図2】

本実施形態のID管理システムで用いるIDタグの一例を示した図である。

【図3】

本実施形態が適用されたID管理システムの概略図である。

【図 4】

図 3 に示す ID 受注端末 3 の機能構成を示す概略図である。

【図 5】

図 3 に示す ID タグ製造工場 4 6 の機能構成を示す概略図である。

【図 6】

図 3 に示す ID 管理端末 5 の機能構成を示す概略図である。

【図 7】

図 3 に示す ID 利用端末 6 の機能構成を示す概略図である。

【図 8】

図 3 に示す ID 管理システムを構成する各装置 3 ～ 6、および 8 のハードウェア構成例を示す図である。

【図 9】

図 4 に示す ID 受注端末 3 の動作を説明するためのフロー図である。

【図 1 0】

図 5 に示す ID タグ製造工場用端末 4 の動作を説明するためのフロー図である。

【図 1 1】

図 6 に示す ID 管理端末 5 の動作を説明するためのフロー図である。

【図 1 2】

図 7 に示す ID 利用端末 6 の動作の概要を説明するためのフロー図である。

【図 1 3】

図 1 2 に示す S 1 6 0 2 (ID 読取手続) の処理の概要を説明するためのフロー図である。

【図 1 4】

図 1 3 に示す S 1 6 1 3 (復号化手続) の処理を説明するためのフロー図である。

【図 1 5】

図 1 3 に示す S 1 6 1 4 (検証手続) の処理を説明するためのフロー図である。

【図 1 6】

図 3 に示す顧客端末 8 の機能構成を示す概略図である。

【図 1 7】

図 6 に示す ID 管理端末 5 の ID 関連情報管理データベース 5 3 に格納される、ID タグ 3 0 0 に関連する管理情報を説明するための図である。

【図 1 8】

図 1 6 に示す顧客端末 8 の動作を説明するためのフロー図である。

【図 1 9】

図 1 2 に示す S 1 6 0 4 （失効手続）の処理の概要を説明するためのフロー図である。

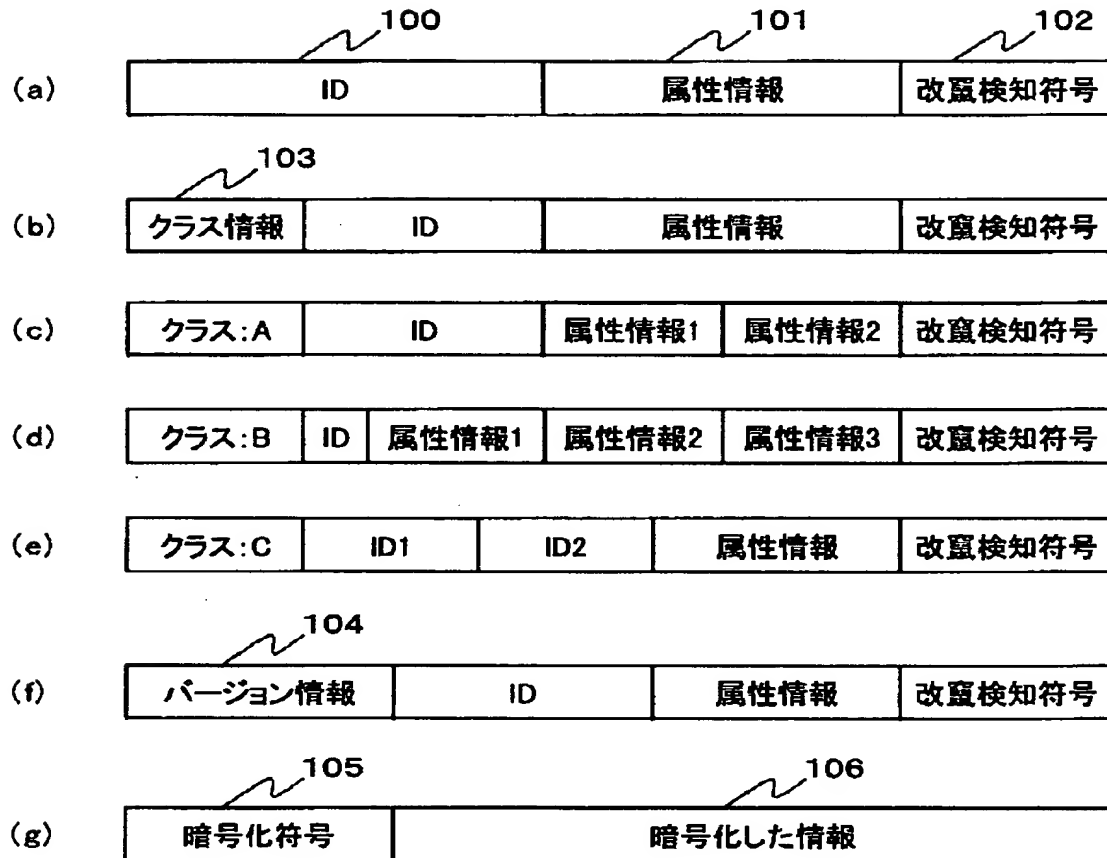
【符号の説明】

1 … ネットワーク, 3 … ID 受注端末, 4 … 製造工場用端末, 5 … ID 管理端末, 1 0 0 … ID, 1 0 1 … ID の属性情報, 1 0 2 … 改竄検知符号, 2 0 0 … 拡張 ID, 3 0 0 … ID タグ, 3 0 1 … 電子回路チップ。

【書類名】 図面

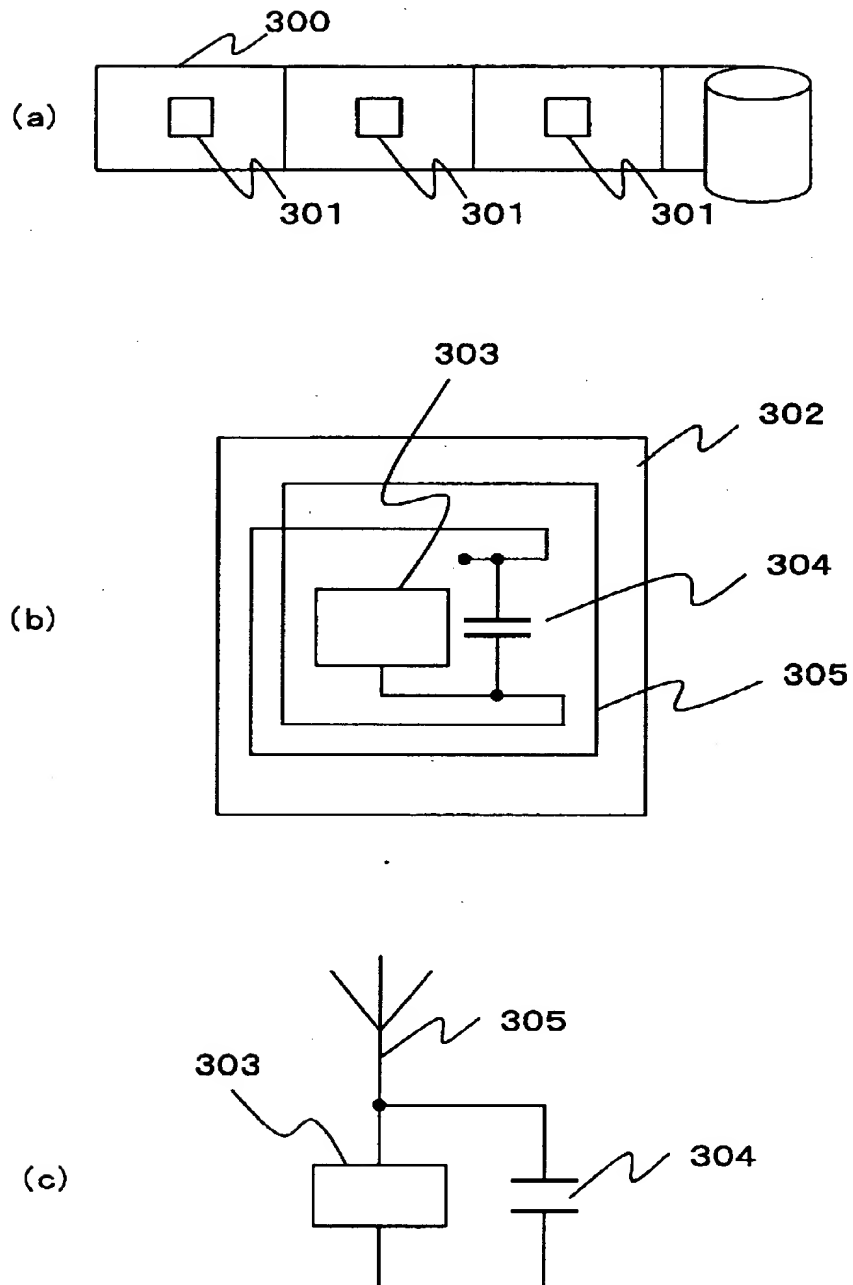
【図 1】

図 1



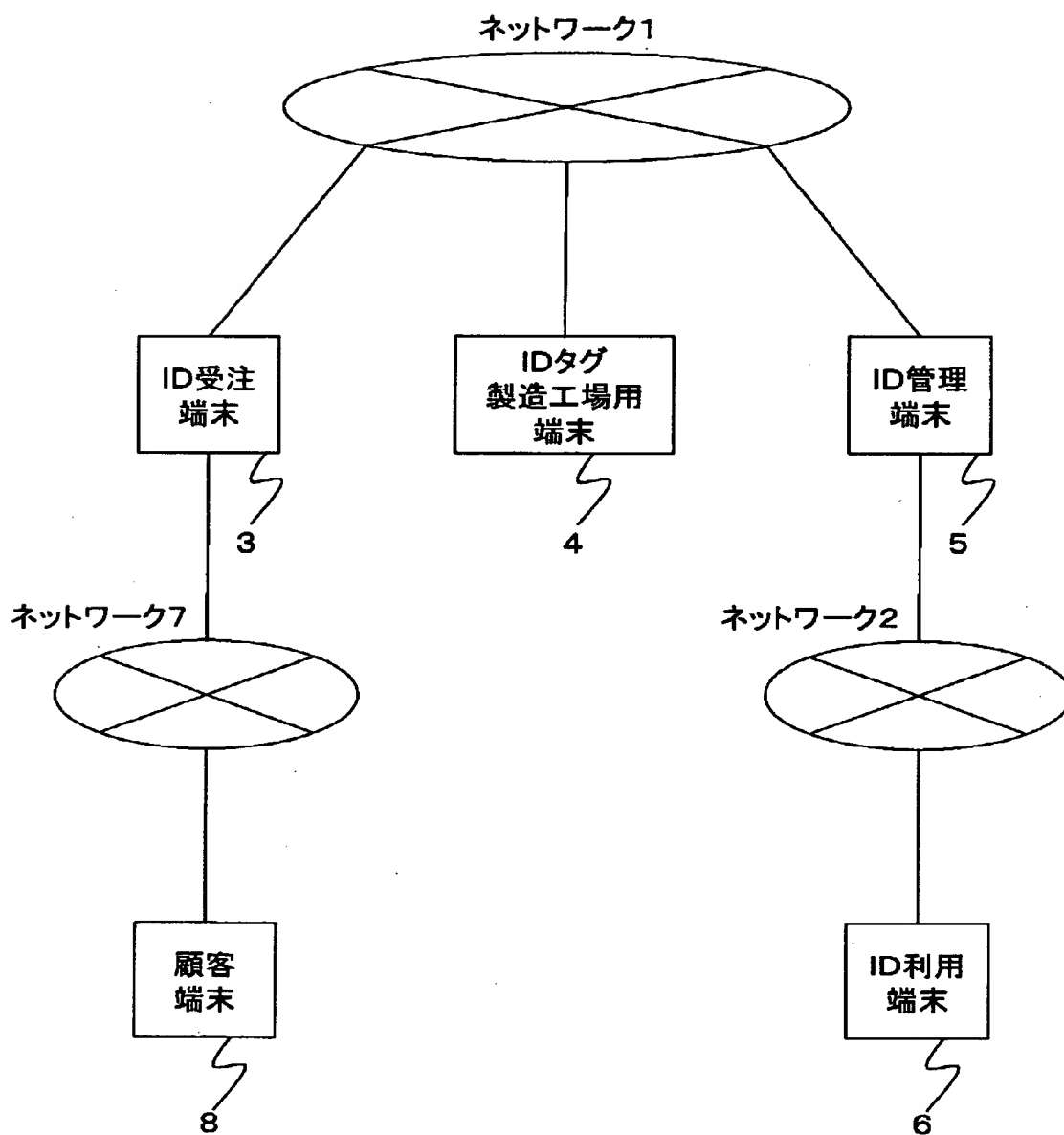
【図 2】

図 2



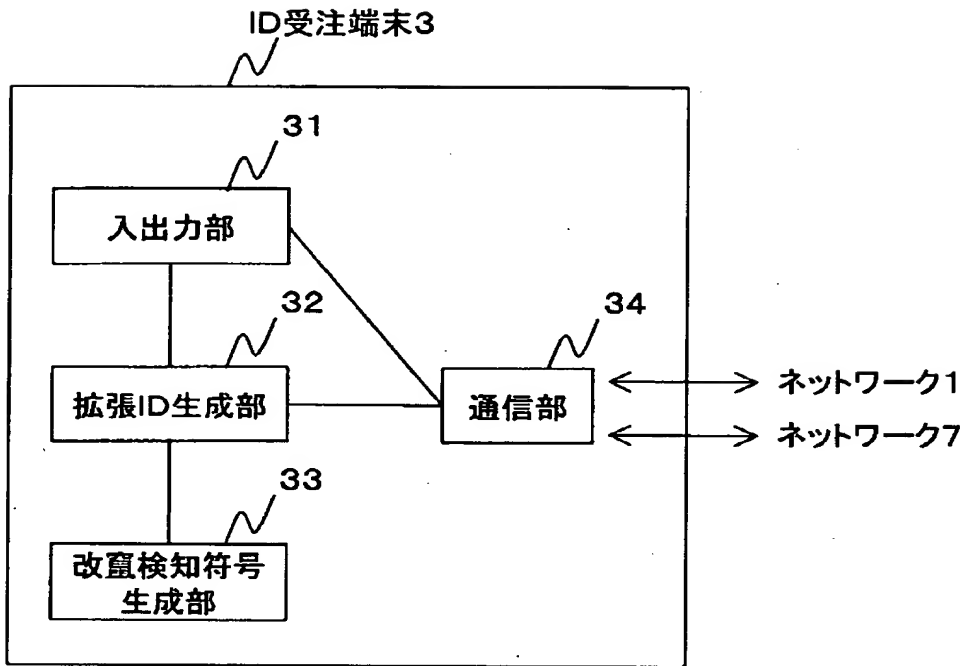
【図3】

図3



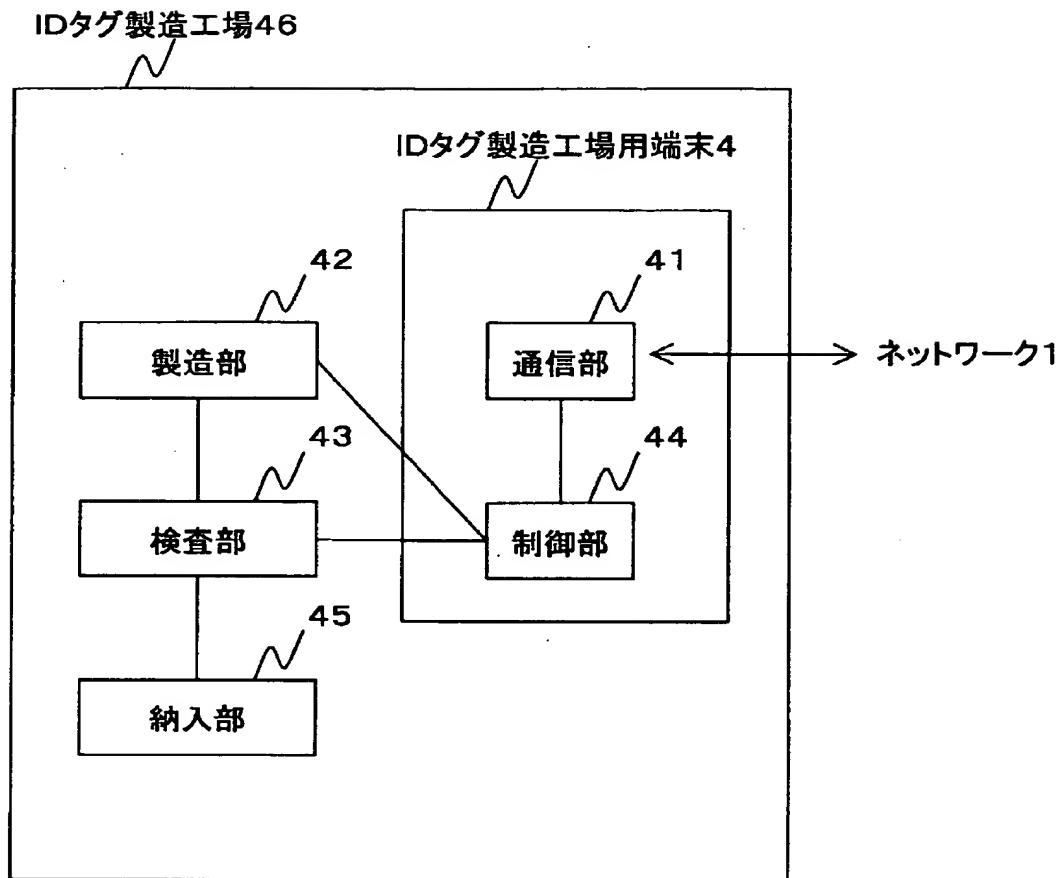
【図 4】

図 4



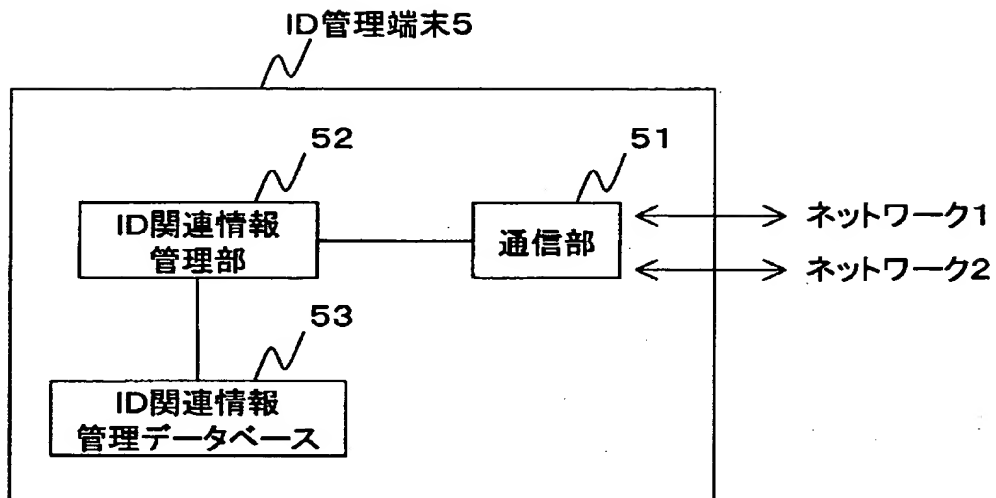
【図5】

図5

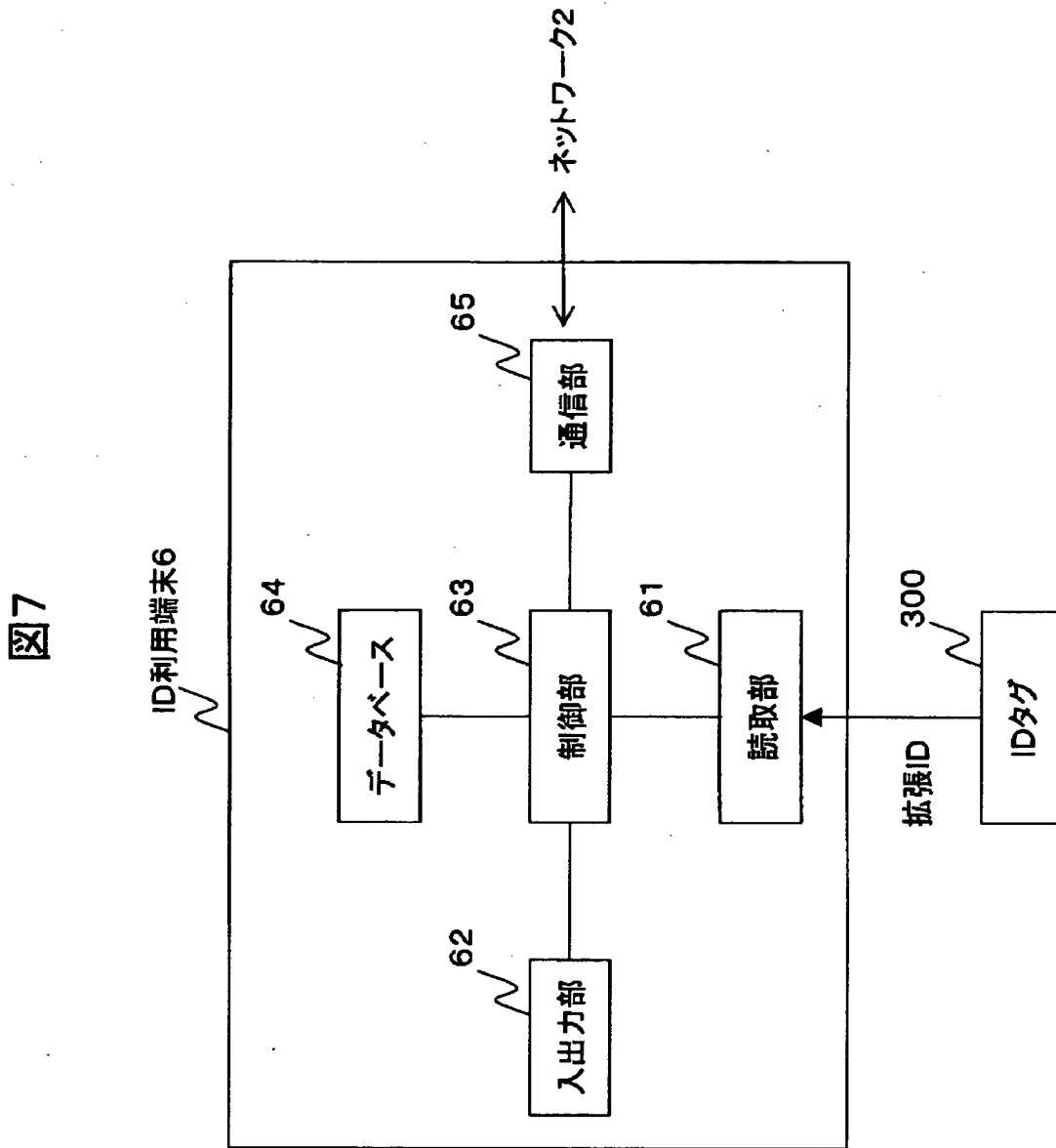


【図 6】

図6

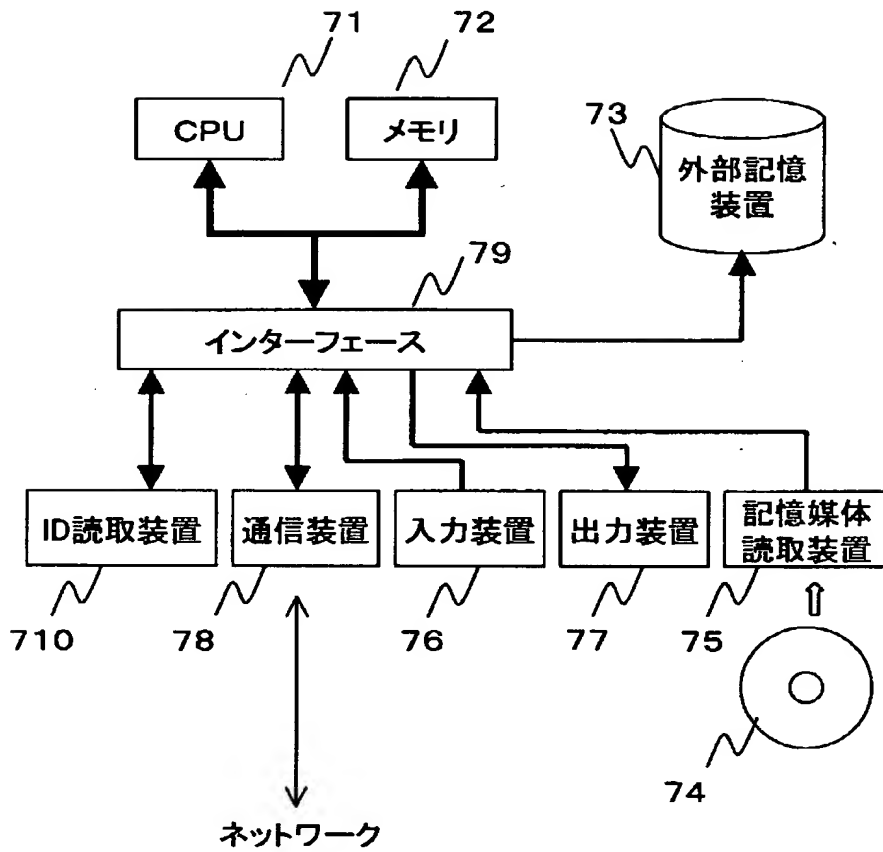


【図 7】



【図 8】

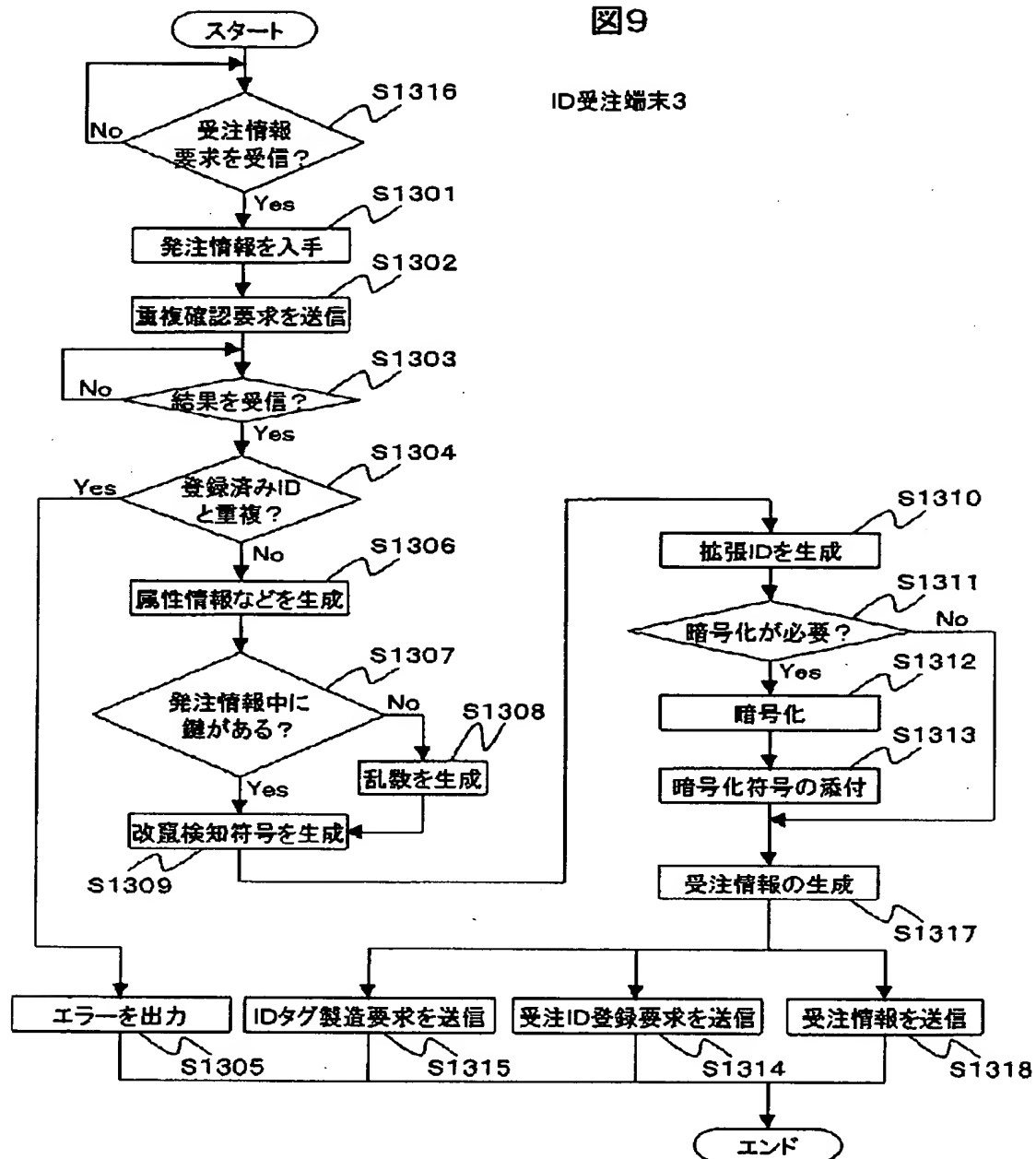
図 8



【図9】

図9

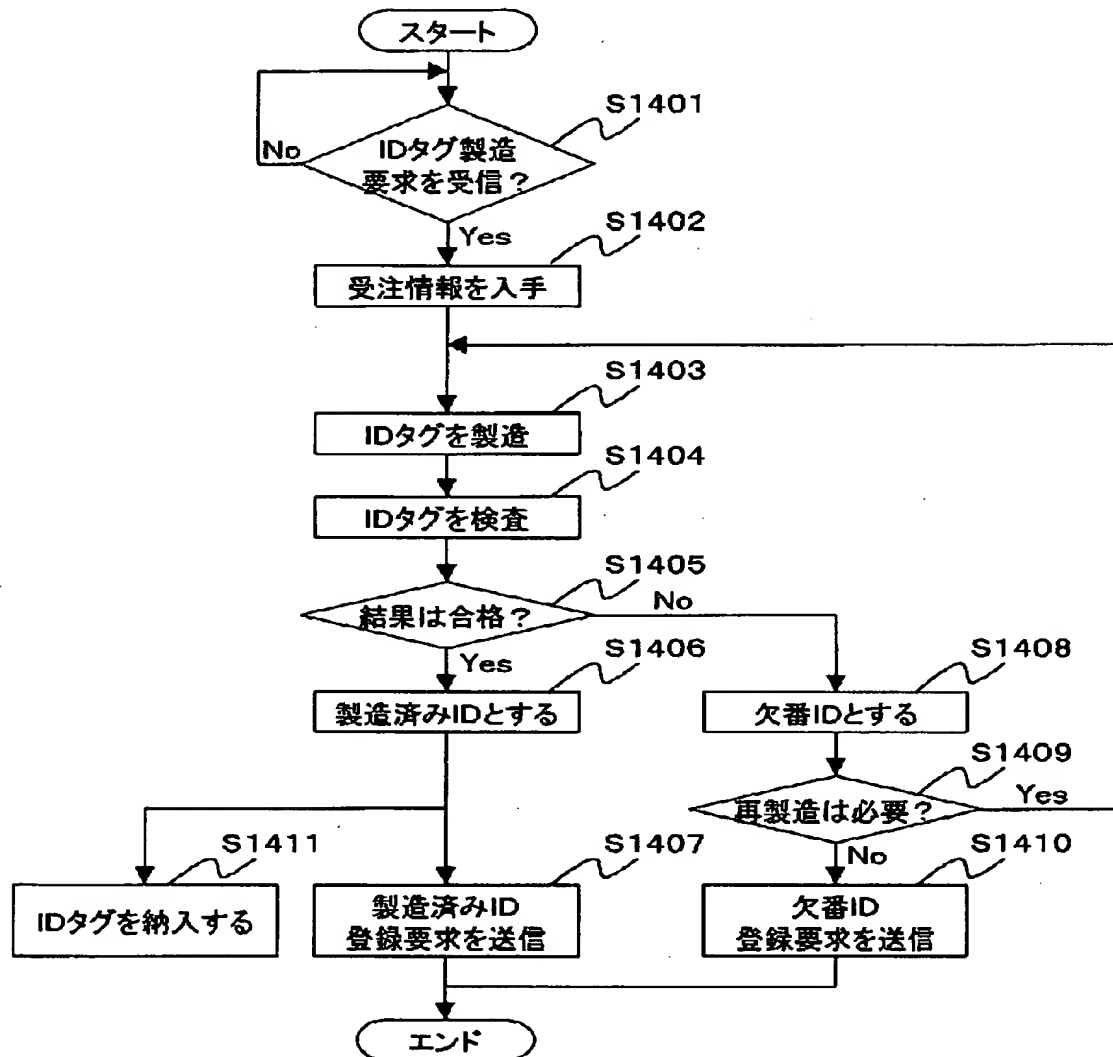
ID受注端末3



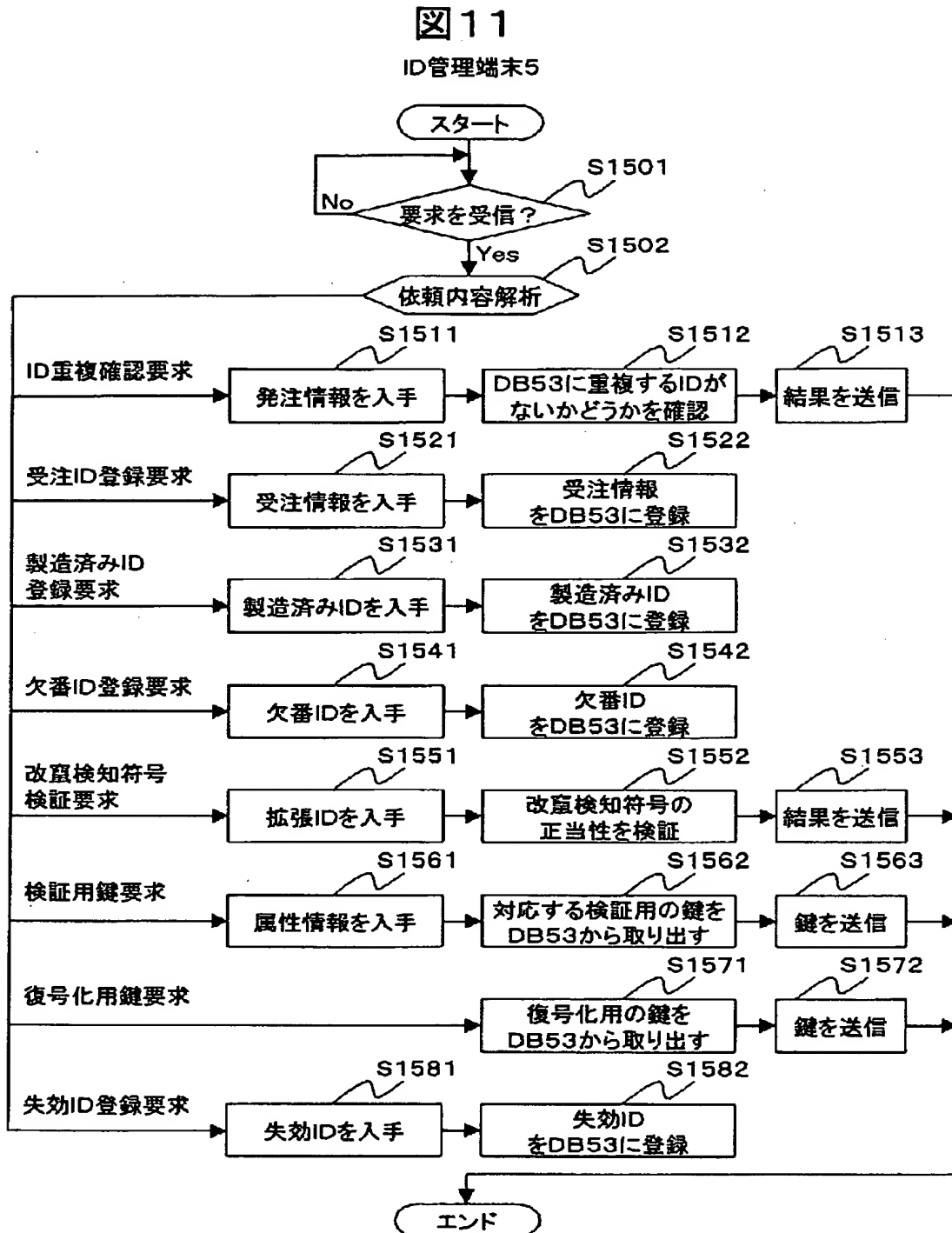
【図10】

図10

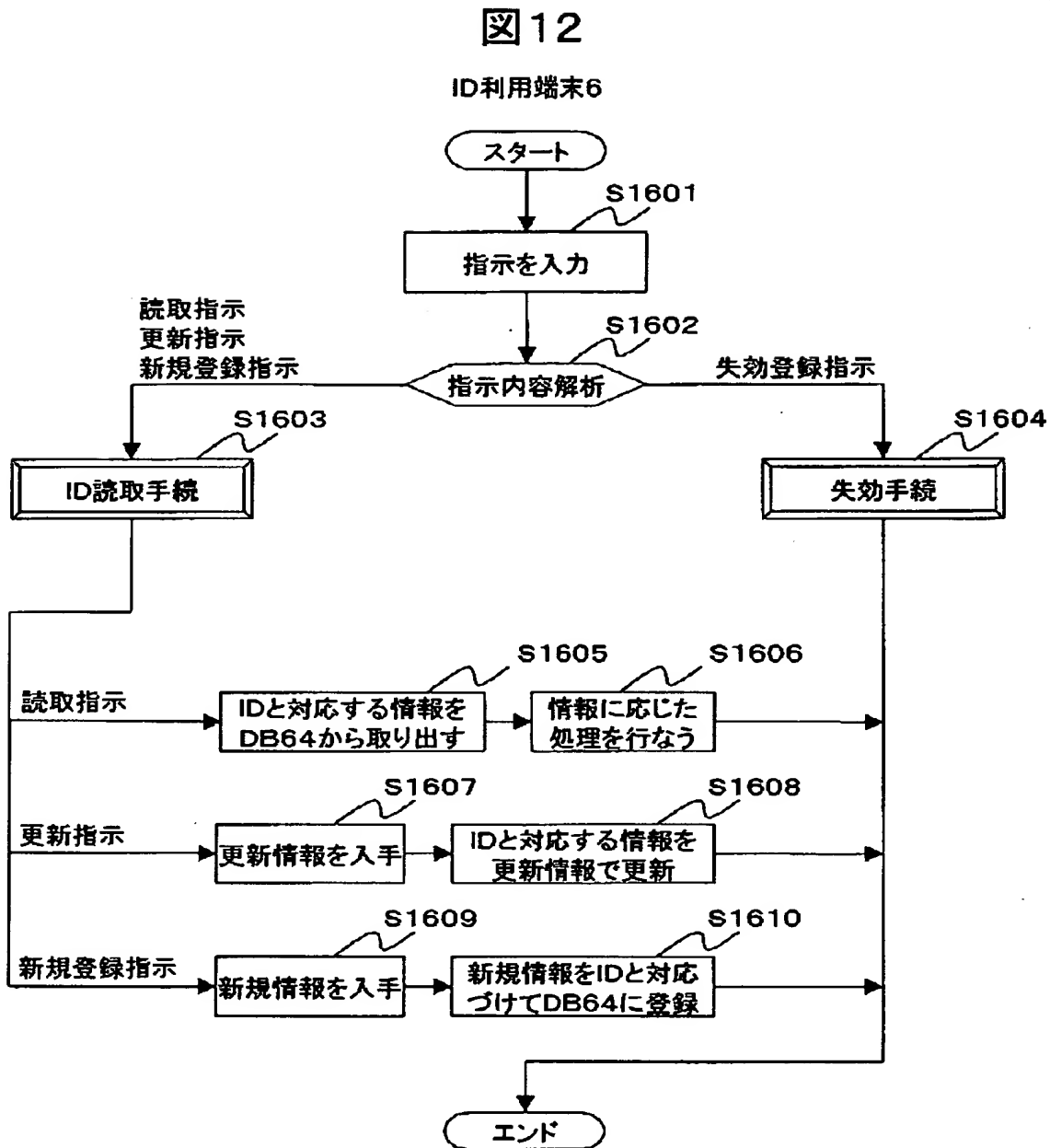
IDタグ製造工場用端末4



【図 11】



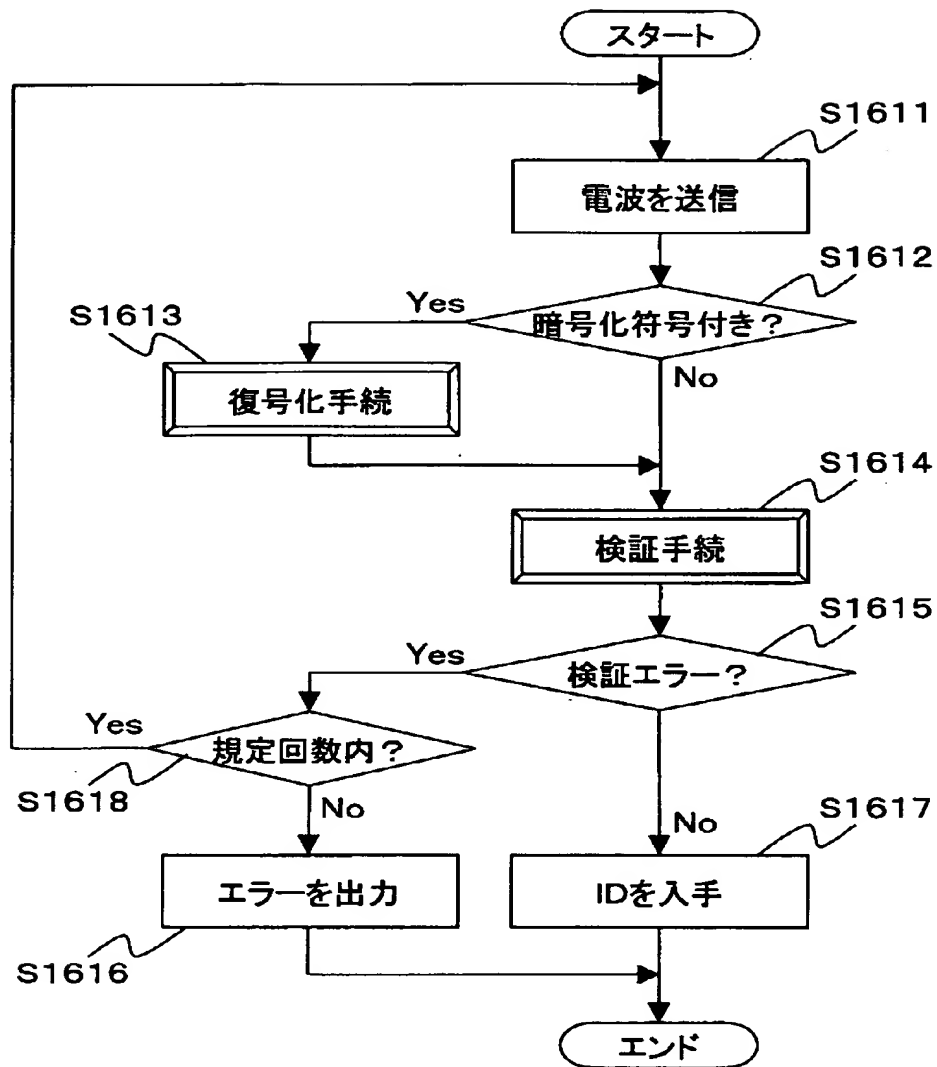
【図 12】



【図13】

図13

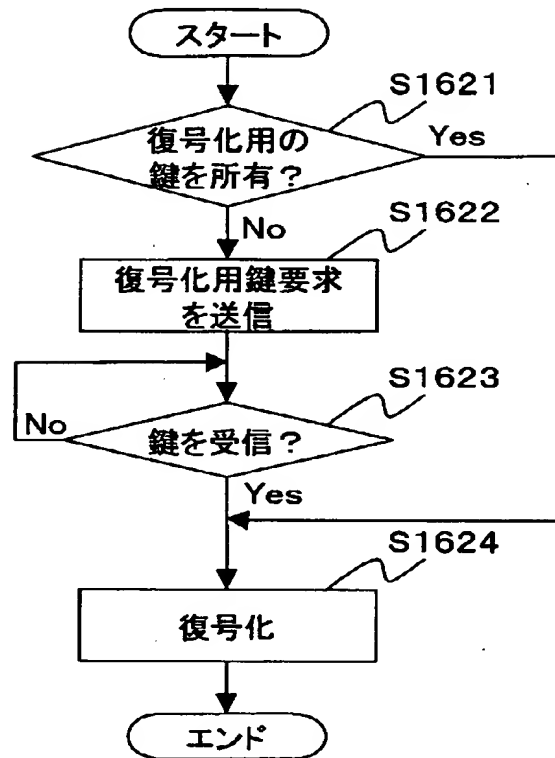
ID読取手続S1603



【図14】

図14

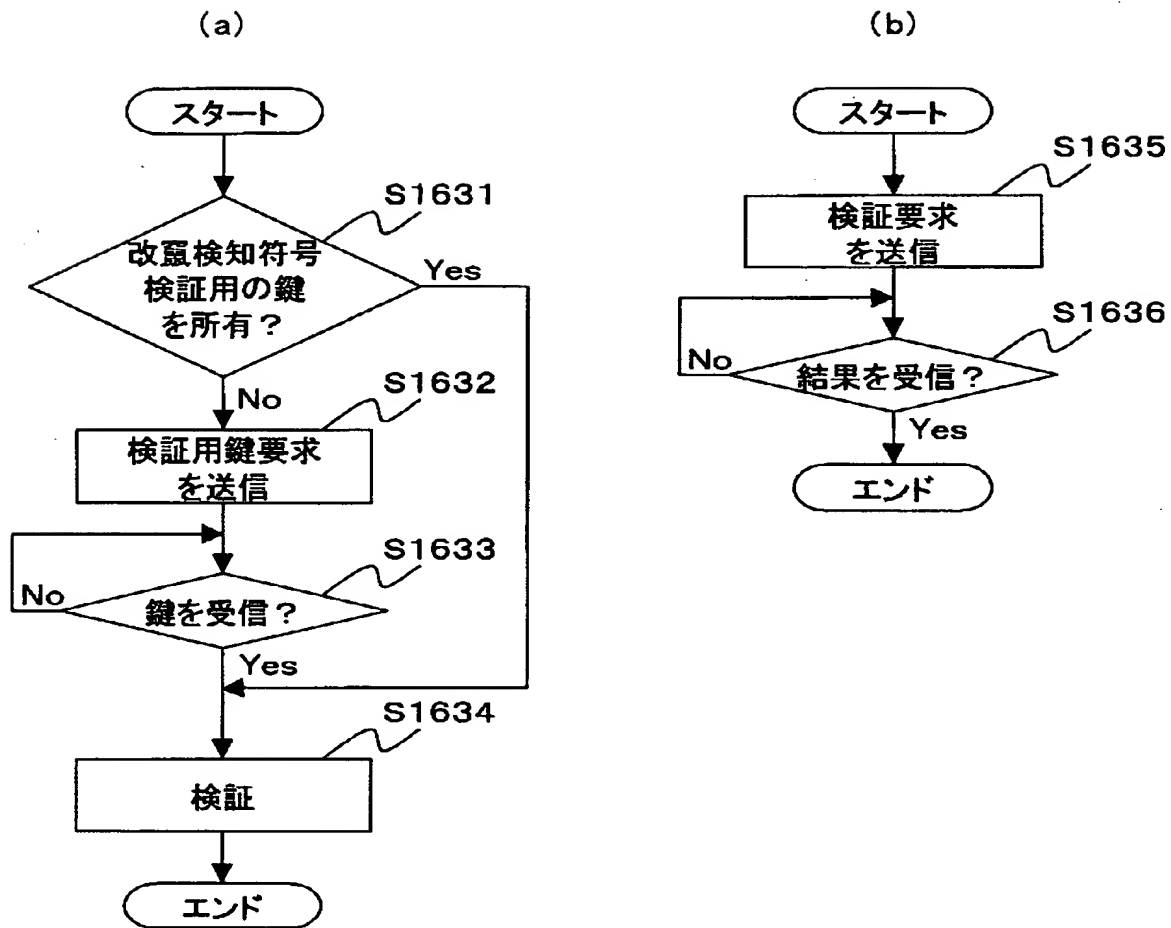
復号化手続S1613



【図15】

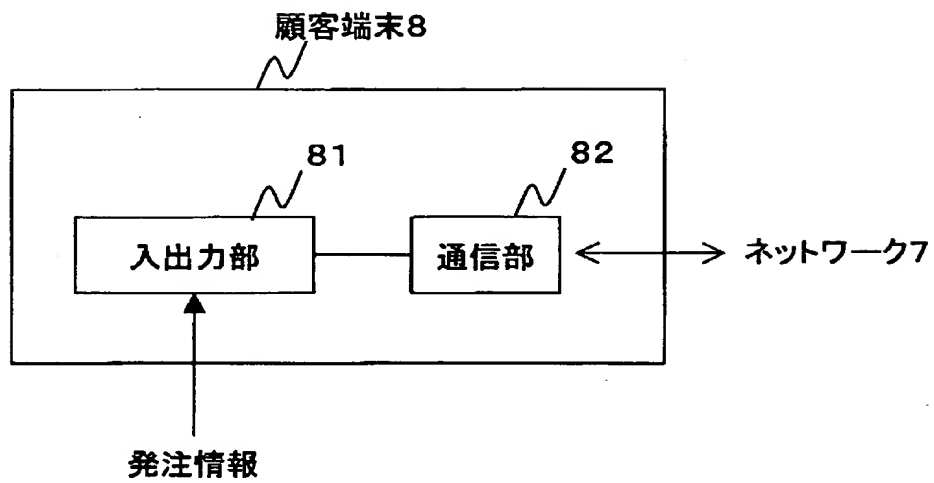
図15

検証手続S1614



【図16】

図16



【図 17】

図 17

ID関連情報管理データベース53

受注情報530

拡張ID200

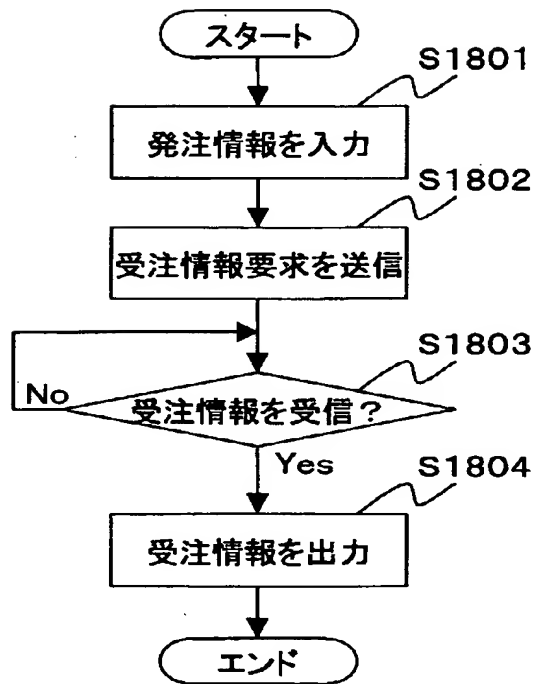
免注情報531

532	533	534	535	536	537	100	101	102	538	539
顧客	個数	条件	納入日	検証用の鍵	番号化用の鍵	ID	属性情報	変更検知符号	発行状況	備考
A社	1	欠番OK	98/07/01	349267	913544	12345624	6801	456123	発行/納入済み	98/06/14 A社納入
A社	—	欠番OK	98/07/01	—	—	23456788	0379	562347	欠番扱い	98/05/28 製造失敗
B社	1	—	00/09/20	824629	886423	7352325188	2886190	527387	製造中	00/08/10 C工場
D社	1	—	98/04/18	837246	—	724498	786439	449728	失効扱い	00/02/07 端末E署名
F社	1000	同一番号	99/12/03	729364	—	497248	369784	497248	発行/納入済み	99/11/29 F社納入
:	:	:	:	:	:	:	:	:	:	:
:	:	:	:	:	:	:	:	:	:	:
G社	1	—	00/03/25	349518	297274	834278	312894	834278	発行/納入済み	00/03/17 G社納入

【図18】

図18

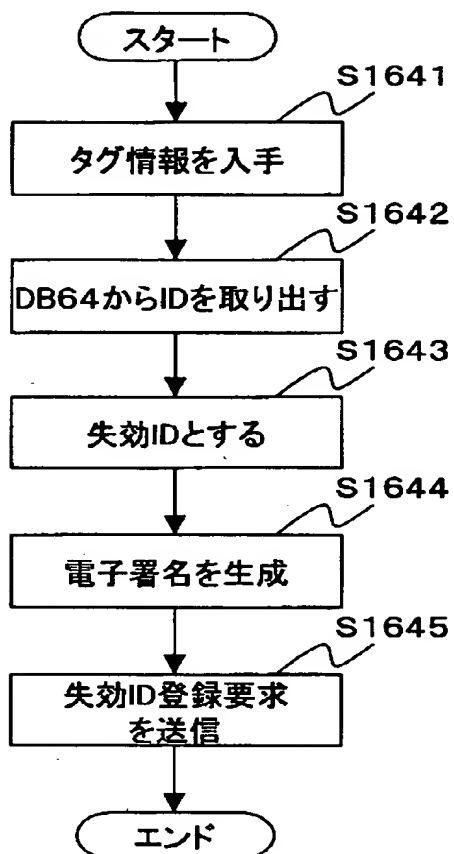
顧客端末8



【図19】

図19

失効手続S1604



【書類名】 要約書

【要約】

【課題】

改竄検知符号を備えたIDの発行と流通を管理し、IDを利用した物品管理を効率よく、かつ、信頼性高く行うことが可能な仕組みを提供する。

【解決手段】

改竄検知符号を備えたIDを書き換え不可領域に格納した電子回路チップをIDタグとして用いる。ID受注端末とIDタグ製造工場用端末の情報をID管理端末に集約し、一括管理する。ID利用端末に機密性の高い情報を格納しておかなくてもいいように、前記情報をID管理端末に問い合わせる、または、前記情報の必要な処理をID管理端末に依頼する手段を構築する。

【選択図】 図3

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地
氏 名 株式会社日立製作所